CREATING A NETWORK MODEL FOR THE INTEGRATION OF A DYNAMIC AND STATIC SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) TEST ENVIRONMENT

THESIS

Marlon C. D. Coerbell, Captain, USAF

AFIT/GCO/ENG/11-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCO/ENG/11-02

CREATING A NETWORK MODEL FOR THE INTEGRATION OF A DYNAMIC AND STATIC SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) TEST ENVIRONMENT

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science

Marlon C. D. Coerbell, BS

Captain, USAF

March 2011

AFIT/GCO/ENG/11-02

CREATING A NETWORK MODEL FOR THE INTEGRATION OF A DYNAMIC AND STATIC SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) TEST ENVIRONMENT

Marlon C. D. Coerbell, BS

Captain, USAF

Approved:

Kenneth M Hopkinson	10 MAR 11
Kenneth M. Hopkinson, PhD, DAF (Chairman)	Date
M. Pachter	10 March, 2011
Meir Pachter, PhD, DAF (Member)	Date
	10 MAR 11
Brett J. Borghetti, Lt Col, USAF (Member)	Date
	10 Mar 2011
Jeffrey W. Humphries, Lt Col, USAF (Member)	Date

AFIT/GCO/ENG/11-02

Abstract

Since 9/11, protecting our critical infrastructure has become a national priority. Presidential Decision Directive 63 mandates and lays a foundation for ensuring that all aspects of our nation's critical infrastructure remain secure. Key in this debate is the fact that much of our electrical power grid fails to meet the spirit of this requirement. My research leverages the power afforded by a federated (combination of) set of simulation tools known as the Electric Power and Communication Synchronizing Simulator (EPOCHS) developed with the assistance of Dr. Hopkinson, et al. Combined with realistic Supervisory Control Data Acquisition (SCADA) traffic models, the power environment is modeled in an electrical simulation environment called PowerWorld©. The network is modeled in OPNET® and populated with sustained, self-similar, network and SCADA traffic by capturing data from a local area network and the Idaho National Laboratory's SCADA network. This research merges both simulators into one working toolset that can realistically model and provide a dynamic network environment coupled with a robust communication methodology. This new suite of tools will enhance the way we model and test hybrid SCADA networks. By combining the best of both worlds (network and power simulation) we get an effective and robust technique that correctly predicts the impact of SCADA traffic on a LAN and vice versa. This ability to properly assess data flows and react to power system transients (faults or abnormal power flows) will allow professionals in the power industry to develop tools that effectively model future concepts for our critical infrastructure.

Acknowledgments

I would like to thank my thesis advisor Dr. Kenneth Hopkinson. His patience and insight was invaluable. I would also like to thank Capt Mark Duncan and Capt José Fadul. Without their help this thesis would not have been possible. Furthermore, I would like to say thanks to Christopher Sheffield. His assistance was critical to developing the methodology for my work. Finally, and most of all, I would like to thank my wife and my two sons. I could not have accomplished this monumental task without their undying love and support.

Marlon C. D. Coerbell

Table of Contents

List of Figures

List of Tables

Page

CREATING A NETWORK MODEL FOR THE INTEGRATION OF A DYNAMIC AND STATIC SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) TEST ENVIRONMENT

I. Introduction

General Issue

Media footage displaying a power generator that was destroyed simply by sending network traffic that disrupted its normal operational cycle, causing the generator to cease functioning due to catastrophic failure was alarming. The public was in an uproar as the 24/7 news cycle ran with this story proclaiming our electrical infrastructure was vulnerable to hackers, or even worse, domestic or international terrorist cells, with the intent of holding America's electric power grid hostage. This may have once been science fiction but now it is too real. A myriad of Presidential Directives, mandates and/or laws have been established proclaiming that our national critical infrastructure must be protected at all costs. In fact, an entire government agency was created with the sole purpose of ensuring that our homeland remains secure. Even though the days of perpetual orange alerts are gone, protecting our networks remains a top priority in all realms of national security strategy.

Compounding the need for security is the fact that our power industry is forever expanding and leveraging new technologies. Smart Grid and micro-grid infrastructure relies heavily on the use of a client-server infrastructure. Our once robust, but proprietary, power networks are no longer capable of supporting the demands of the network traffic that's needed to support this capability. Utility companies are forced to use the Internet to help manage and distribute power throughout the continental United States. This methodology, while robust, puts our once secure (by detachment alone) power infrastructure in close proximity to every

vulnerability lurking in the World Wide Web. We can no longer expect our critical infrastructure to remain secure while it is exposed to the wild.

Problem Statement

Many power companies are in the process of researching how they can take advantage of the additional bandwidth that can be gained by adding thousands of miles of already existing power lines to the Internet. Not only can, Institute of Electrical and Electronics Engineers (IEEE) standard P 1901, the latest broadband over power line standard, provide bidirectional communication between the power company and their hardware, they also hope to provide that very same connectivity to their customers. [1] While this endeavor seems promising, one wonders how they can continue to leverage these capabilities (building Smart Grid infrastructure and providing Internet connectivity to every home) while ensuring their own private and corporate infrastructure remains safe. In fact, maintaining the security of our nation's power supply mandates that this question be answered.

A methodology of this scale demands robust planning. The utility industry has to be able to adequately plan and forecast demand, power distribution and the need for robust and secure communication protocols. Often times one is able to model networks or power, but finding a suite of tools that models all aspects of the modern power grid infrastructure is quite difficult. Likewise, coupling disparate suites of simulation technologies and simultaneously developing a plan that ensures that our electric infrastructure remains secure is no easy task. The myriad of electric protocols, network protocols and the simultaneous need to provide the logic to be able to communicate and solve the vast array of transient malfunctions that occur during normal power operations makes it difficult to generate the toolset that is needed to accurately and adequately model modern power grid infrastructure. Only through accurate models can we ensure that our

critical infrastructure remains sound. Although we do have a suite of tools that come close to achieving a sound balance, none is able to leverage the use of agent architecture to maintain trust, correct malfunctions in power and communications, provide the ability to scale to appropriate size and incorporate real and/or simulated components.

Research Objectives/Questions/Hypotheses

The purpose of this research is to develop and execute a methodology for federating (or combining) power and network simulation software. Once established, this proof of concept will give rise to a toolset, providing the necessary ability to develop and test not only a myriad of power and communication infrastructure, but all manner of equipment (hardware and/or software) and the means to secure it.

Through this research, the toolset can facilitate the resolution of several rudimentary questions. Can a power network, in the presence of extraneous network traffic, provide the necessary throughput to solve power grid malfunctions in a timely manner? At the same time, can it sustain critical communications amongst every node in the network? Answering these two questions is critical to determining if power networks can successfully coexist with corporate and public local area network traffic?

It is the author's belief that a federated suite of tools can lay the groundwork for the development of a sound approach, guaranteeing that the utility industry maintains the capability to plan for future network expansion. This technique co-optimizes both network communications and the ability to quickly resolve power grid malfunctions; returning the grid to a previously, known, stable state.

Research Focus

The focus of this research is the electric utility industry. More specifically, the expansion of existing power utilities that choose to, or have chosen to, develop and/or incorporate the use of Smart Grid and micro-grid technologies to take full advantage of bidirectional (industry to consumer and vice versa) corporate and public networks.

Investigative Questions

This research hopes to answer several questions

1. Can OPNET® and PowerWorld© be used to develop a simulation tool that models existing power grid infrastructure?
2. Can this same tool maintain pre-established benchmarks, resolving power grid malfunctions in the presence of elevated background traffic?
3. Can this tool scale, modeling complex power and communication networks, while simultaneously returning malfunctioning power infrastructure to steady state within these very same guidelines?

Methodology

Existing communication and power simulation environments were federated to develop both the power and network environment. The power environment was modeled off of existing IEEE power cases and the network environment was modeled to support a suite of protocols and nodes that mirror the location and number of power buses. A C++ simulation manager was developed to control and build the simulation. Software agents were deployed in the communication environment to act upon and recommend corrections to the anomalies injected into the power scenario.

The simulation was run and several statistics were measured to detect network delay and the viability of existing software agents.

Assumptions/Limitations

The communication suite was chosen to utilize the already existing capability to capture and provide the appropriate statistics. Background network and power traffic was developed to be generic in nature and does not succinctly model all the disparate transactions that exist on a "real" network. In addition, traffic load was modeled off of specific locations and timeframes and will not adequately represent all existing LANs at all hours of the day. In addition, power communication protocols were modeled using packet payload and not identical representations of every packet flowing through the network: in particular MODBUS and DNP3 protocols. Most important of all, our power simulator was not capable of handling a dynamic, transient environment. Time was solely handled by the communication environment. It is hoped that this could be remedied in future releases of the software and followed up in future work.

Implications

It is hoped that this federated environment will provide the capability to adequately model future Smart Grid and micro-grid migrations and/or installation and prove that, not only is this infrastructure shift feasible, but utility industries can safely leverage the additional bandwidth provided by upgrading their infrastructure while simultaneously ensuring that they have the capability to establish an affordable and safe security posture.

Preview

Chapter two briefly describes the history of SCADA, the two main communication protocols used by the power industry and the two main power grid constructs. It also describes

the existing suite of federated simulation environments along with their strengths and weaknesses.

Chapter three describes the methodology for creating this federated simulation environment.

Chapter four lays out the results of the implementation, in particular the methods used to deploy both the 14 and 145 node cases.

Finally, chapter five lays out a detailed conclusion and focuses on the different aspects/possibilities for future work regarding existing simulation engines and the development of additional tools and scenarios.

II. Literature Review

Chapter Overview

The purpose of this chapter is to present relevant background and existing research to the reader. This material is the foundation for developing investigative questions, assumptions and direction for formulating and conducting this thesis work.

Description

Supervisory Control and Data Acquisition (SCADA)

A standard power grid is managed via several automated systems. In particular, SCADA systems have been used to monitor the Utilities industry since the 1960s [2].

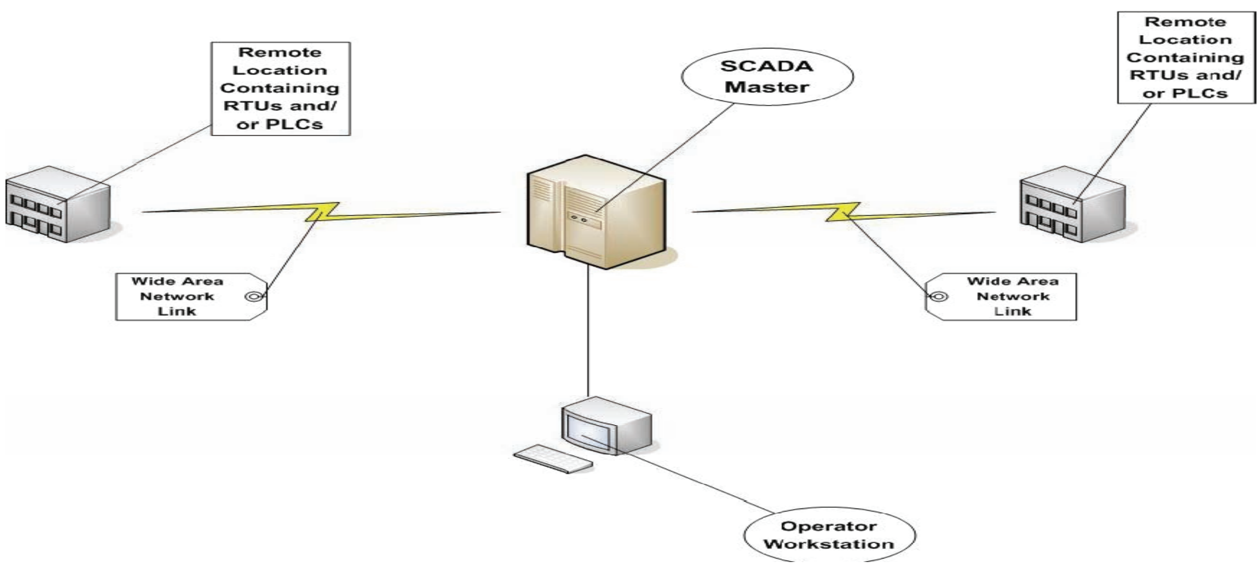


Figure 1. Typical SCADA system [2]

Figure 1 depicts a standard SCADA environment. Field data interface devices communicate directly with the remote telemetry unit (RTU). This unit is used to "convert electronic signals

received from field interface devices into the language (known as the communication protocol) used to transmit the data over a communication channel." [2] Programmable logic controllers (PLCs) also couple with field interface devices and are virtually interchangeable with RTUs. Local control programs that were historically stored in PLCs are now integrated in RTUs while the communication modules that transferred the state of the control program that were native to RTUs were integrated within PLCs [2]. Hence, you essentially have the same device providing the interface for the supervisory control function within the SCADA system.

The communications architecture for the network can consist of cable (coaxial, Cat III/V/Ve, fiber), telephone (POTS, ISDN, T1…, DSL) or radio (microwave, wireless). These networks have traditionally been dedicated to control traffic only, but with the ubiquity of Local Area Networks (LANs), Wide Area Networks (WANs), MANS (Metropolitan Area Networks (MANs), Wireless Local Area Networks (WLANs) the high cost of such a network is no longer practical. Additionally, it has become increasingly attractive to be able to integrate "SCADA data with existing office applications, such as spreadsheets, work management systems, data history databases, Geographic Information System (GIS) systems, and water distribution modeling systems." [2]

The central host computer or the SCADA master is one of the most critical device/s in the SCADA network. These machines provide the ability for the operator to communicate with and monitor remote devices via a networked human/machine interface or HMI. The communication protocol is passed back and forth, between man and machine and the master. This was traditionally displayed and rendered with proprietary hardware and operating systems. No longer the case, vendors have migrated their platforms to reside on standard personal computers and servers, drastically reducing the cost to implement and/or expand these networks.

Workstations/end stations are now able to readily interface with the central computer; however the software, for the most part, remains proprietary and can implemented at a significant cost. Migration to commercial of the shelf (COTS) software is sometimes feasible, but typically this methodology tends to focus on compatibility with a variety of equipment and instrumentation not implementation of the SCADA system itself. [2]. Table 1 lists the software products that are typically used with a SCADA system.

Table 1. Software products typically used within a SCADA system [2]

APPLICATION	PURPOSE	PLATFORM
Central host computer operating system	Used to control the central host computer hardware	UNIX©, Windows©, etc.
Operator terminal operating system	Used to control the central host computer hardware	UNIX©, Windows©, etc.
Central host computer application	Handles the transmittal and reception of data to and from the RTUs and the central host. Provides the graphical user interface which offers site mimic screens, alarm pages, trend pages, and control functions.	Proprietary/vendor specific
Operator terminal application	Enables users to access information available on the central host computer application	Proprietary/vendor specific
Communications protocol drivers	Required to control the translation and interpretation of the data between ends of the communications links in the system	Proprietary/vendor specific
Communications network management software	Required to control the communications network and to allow the communications networks themselves to be monitored for performance and failures	Proprietary (older systems)/COTS (modern systems)
RTU automation software	Allows engineering staff to configure and maintain the application housed within the RTUs (or PLCs)	Proprietary/vendor specific

Historically, SCADA networks took on the mold of three distinct architectures. The first was a basic stand-alone system that had limited functionality (see Figure 2). This model relied on main-frame computers and the networks and their proprietary protocols were designed to communicate with RTUs only. “Connections to the master typically were done at the bus level

via a proprietary adapter or controller plugged into the Central Processing Unit (CPU) backplane.” [2] What limited redundancy existed was due to the fact that two identical main-frames (one live and the other hot-swappable) were directly connected to the system. Unfortunately, this meant that in the event of a detected failure, the system would go off-line until the backup computer could be brought on-line.

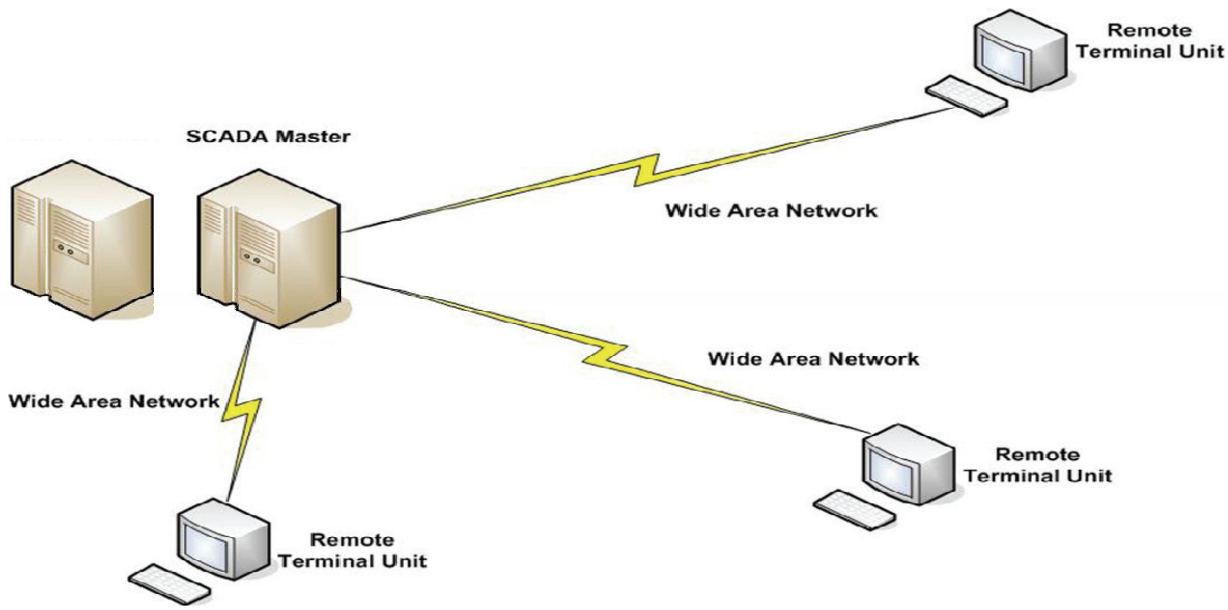


Figure 2. First Generation SCADA Architecture [2]

The next generation of SCADA systems took advantage of technology that were able to leverage system miniaturization and LAN technology. [2] These smaller and cheaper computers were distributed in a sense that they each had specific roles and in the case of a failure, could readily take on the role of the malfunctioning station. Since the LAN protocols being used were still proprietary in nature, vendor specific SCADA systems were still unable to communicate with similar systems made by other companies. Figure 3 is a basic representation of such a system.

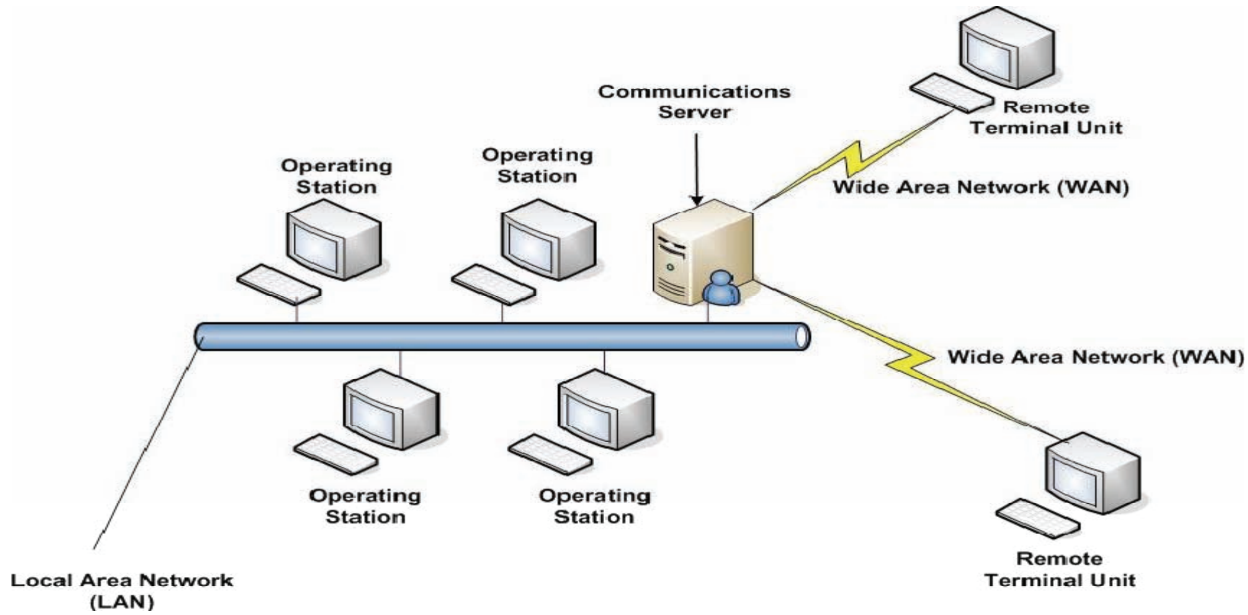


Figure 3. Second Generation SCADA Architecture [2]

Finally, the current version of SCADA systems takes on a true networked architecture. This system still shares master station functions, has vendor proprietary protocols with RTUs and PLCs, but it has an open architecture that uses open standards and protocols that no longer restrict SCADA functionality on a LAN. [2] WAN protocols like Internet Protocol (IP), Universal Datagram Protocol (UDP) and Transport Control Protocol (TCP) allow vendors to create remote devices that are able to communicate over long distances to various master stations. This expands on the limited redundancy gained in second generation systems by adding redundancy that practically eliminates the loss of an entire system in the event of failure in any one location. Figure 4 on the following page displays a network that is comprised of three disparate locations.

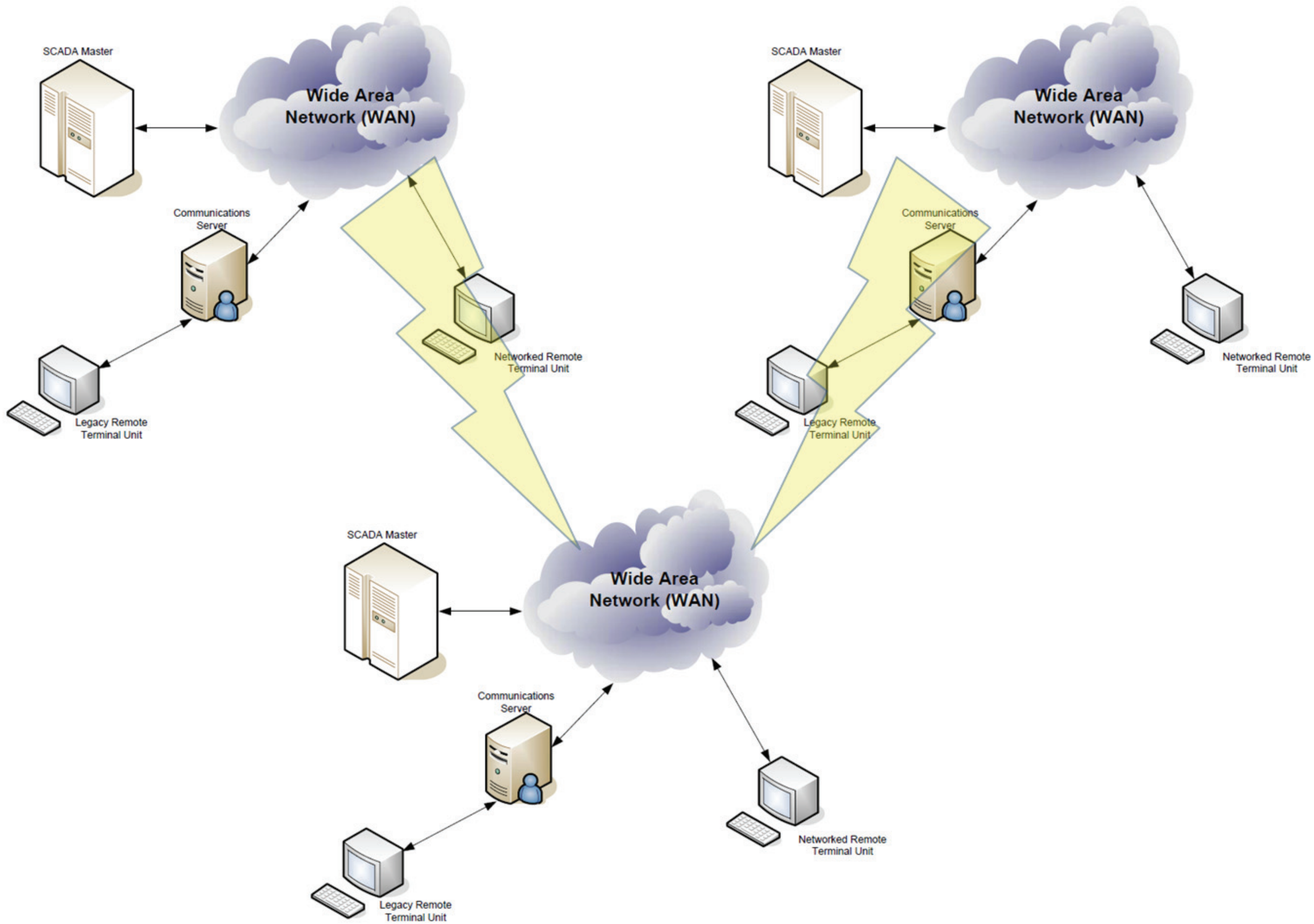


Figure 4. Third Generation SCADA Architecture [2]

SCADA Protocols

Primarily, current SCADA systems utilize several communication protocols, but the most popular are the MODBUS and Distributed Networking Protocol (DNP). MODBUS, developed by Modicon in 1979, is the older of the two protocols and was originally released "as a simple way to transfer data between controls and sensors via RS-232 interfaces," [but now it also] supports other communication media, including TCP/IP." [3] This newer version of MODBUS has been incorporated into the International Electrotechnical Commission (IEC) 60870-5 (Telecontrol equipment and systems), 61158 (Industrial communication networks - Fieldbus specifications) and 61784-2 (Industrial communication networks - Profiles) standards. The original MODBUS protocol resided at the application, data link and physical layer of the OSI model (Figure 5), communicated between vendor developed PLCs and master stations (client/server) and primarily used serial connections as the communication medium. Today the MODBUS protocol, via an integrated TCP/IP extension (Figure 6), is much more flexible. Still utilizing a client/server construct, it now uses layer one, two, three, four and seven to communicate over several different physical layers (serial and Ethernet) [4].

Layer	ISO/OSI Model	
7	Application	MODBUS Application Protocol
6	Presentation	Empty
5	Session	Empty
4	Transport	Empty
3	Network	Empty
2	Data Link	MODBUS Serial Line Protocol
1	Physical	EIA/TIA-485 (or EIA/TIA-232)

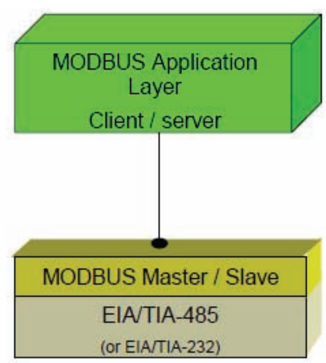


Figure 5. Original MODBUS Specification [4]

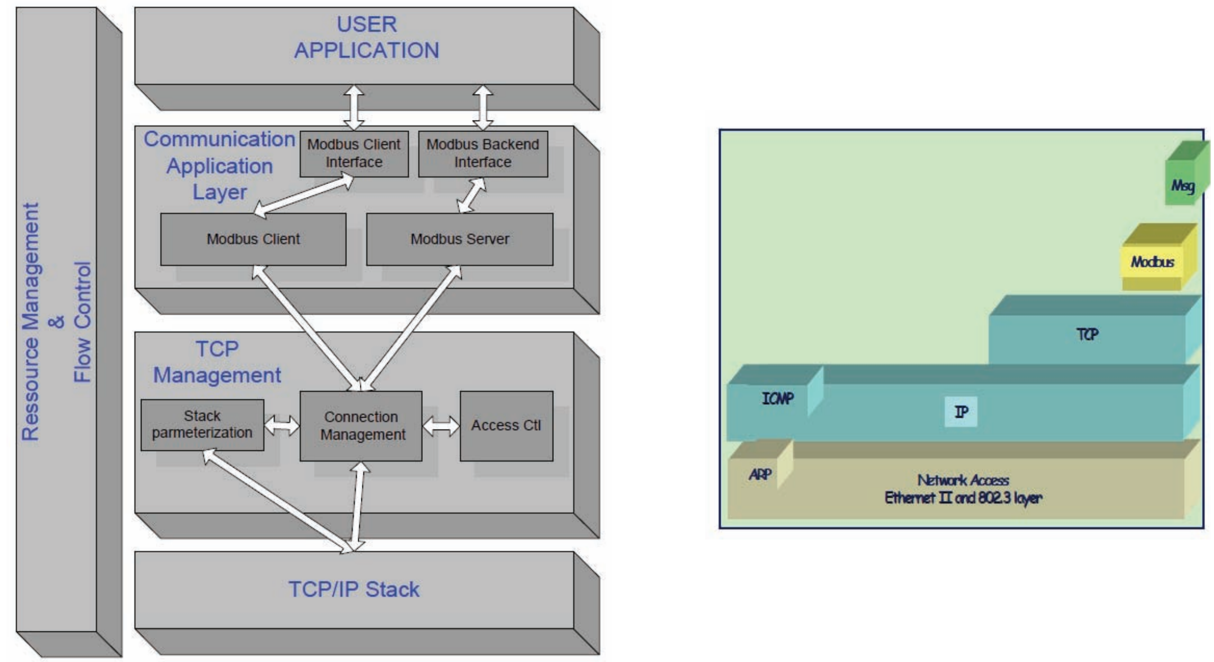


Figure 6. Current MODBUS Protocol [5]

The client server model is based on four types of messages:

- A MODBUS Request is the message sent on the network by the Client to initiate a transaction,
- A MODBUS Indication is the Request message received on the Server side,
- A MODBUS Response is the Response message sent by the Server,
- A MODBUS Confirmation is the Response Message received on the Client side [4]

The next class of SCADA protocols is DNP or DNP 3.0 Basic 4 to be exact. DNP was originally released by Westronic, Inc. (now GE Harris) in 1990 with DNP3 to follow in 1993 [3]. Like MODBUS, DNP3 is a protocol used to transfer data between two devices over varying physical mediums. This protocol utilizes layer one, two, a “pseudo-transport layer [three that] segments application layer messages into multiple data link frames,” and an application layer (layer seven). [6] Utility companies are not constrained by the need to use proprietary hardware

because this protocol is an open standard. This communication models the client/server architecture by establishing the transfer of requests and or responses between master and outstations and was specifically created to facilitate “conversations” in a SCADA environment. DNP3 data types consist of arrays that mimic logical representations of system state or Boolean devices and the binary “[v]alues in the array represent input quantities that the outstation measured or computed.” [7] This information is stored in databases located in the master and outstations. High data integrity is maintained via a confirmed service in the application and data link layers. DNP3 can support several modes: polled only, polled report-by-exception, unsolicited report-by-exception (quiescent mode) and a mixture of modes one through three. [2] Altogether, minimal overhead and an open standard is the driving force behind the popularity of DNP3.

In addition to basic differences in data types, there was also a study done to compare communication efficiencies between MODBUS and DNP3. In a white paper written by Control Microsystems, the author claims “[b]y utilizing DNP3 it is possible to significantly reduce bandwidth on your communication channels, allow more devices to be added to your system (i.e. scalability), and add new functionality to devices, such as time stamping.” [8] The methodology for the experiment is listed in Table 2.

Table 2. MODBUS vs. DNP3 Experiment [8]

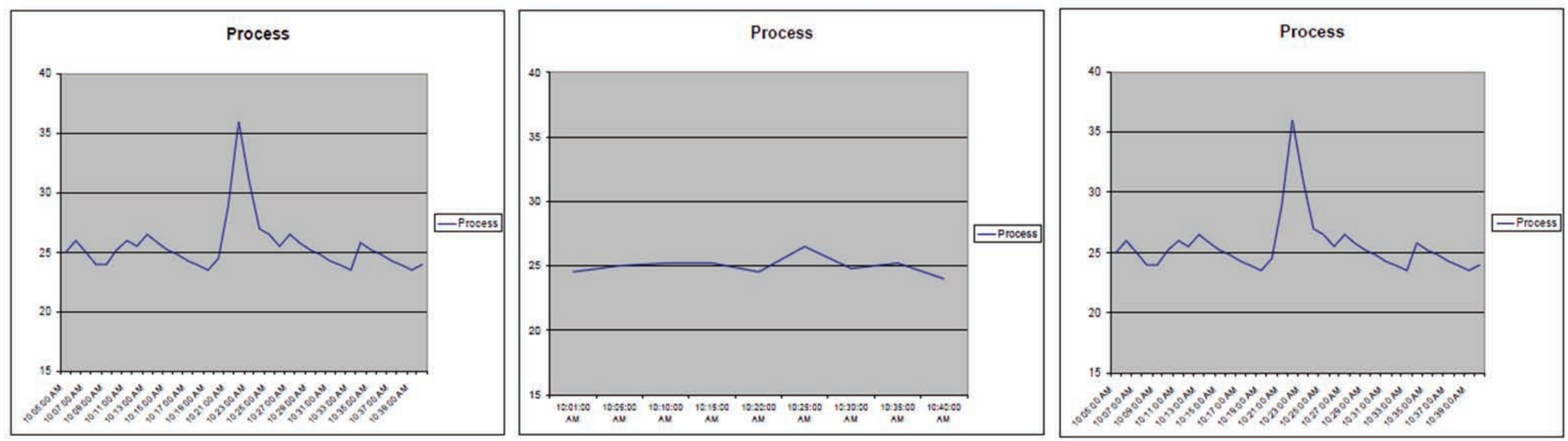
Device	Requirements	Assumptions
32 Digital Inputs/Registers	Log changes with a timestamp accurate to the nearest 10 secs	128 digital input changes/hr
16 Analog Inputs/Registers	Digital changes need to be reported within one minute	80 analog input changes/hr
	Analog changes need to be reported within 10 mins	No packets are dropped

The author of the white paper used two methods to configure the MODBUS registers. The first, used 17 bytes/10 seconds for 32 status registers and 45 bytes/10 seconds for 16 input registers - 62 bytes/10 seconds. The second method placed 32 digital inputs into two input registers and kept the 16 analog input registers for a total of 18 registers - 49 bytes/10 seconds. DNP3 is able to take advantage of timestamps, polling intervals of one minute and 10 minutes respectively and an integrity poll every hour.

Table 3. MODBUS vs. DNP3 Experiment [8]

Methodology	**Results**
MODBUS 1: 62 bytes per poll x 6 polls every minute x 60 minutes x 24 hours	535,680 bytes/day
MODBUS 2: 49 bytes per poll x 6 polls every minute x 60 minutes x 24 hours	423,360 bytes/day
DNP3 Integrity: 100 bytes per poll x 24 hours Analog Events: 256 bytes per poll x 5 polls every hour x 24 hours Digital Events: 247 bytes per poll x 4 polls every hour x 24 hours Empty Polls: 35 bytes per poll x 50 polls every hour x 24 hours	2400 + 30,720 + 23,712 + 42,000 = 98,832 bytes/day

The final results listed in Table 3 show that DNP3 is 4.28 times more efficient than the best MODBUS scheme. A similar study by MultiTrode, a SCADA technology company, reinforces the need to utilize the date and timestamp feature. If the device fails, further analysis can be captured once it is brought back on-line. In addition, instead of the master telemetry unit (MTU) polling every remote telemetry unit (RTU) via the MODBUS protocol, these same devices, when using DNP3 need only receive the changes instead of all data/event from all registers. This inundation of data and events unintentionally masks the true environment. Figure 7 displays the results of this study.



Real Data　　MODBUS Protocol　　DNP3 Protocol

Figure 7. MODBUS/DNP3 Protocol Study [9]

Grid Topologies

Power grids have evolved since the 1970s and 80s. The construct laid out in figure one has become systematically more complex. The 1990s gave rise to distribution systems that leveraged the yearly increase in computer power and the rise of robust communication networks. As of late, the two most advanced power grid schemas are Smart Grid and Microgrid technologies. While both rely on a decentralized and distributed management system and the potential for bi-directional power flow, they do have some significant differences.

Currently, microgrid definitions are still in flux but it is generally defined as “a variety of distributed generators, distributed storage devices, loads, supervisory control and protection systems; it is flexible and dispatchable, namely it could operate in grid-connected or stand-alone mode and could switch between the two modes seamlessly by using static switches; it can provide both thermal and electrical energy to consumers via cooperation of related devices; the capacity of a microgrid is generally between kilowatts and megawatts; and it is interconnected to low or middle level distribution networks.” [10] Manufacturers of grid technology also need to overcome the challenge of maintaining affective communication amongst devices with varying degrees of response. New protocols need to be established to address this issue. In particular the Institute of Electrical and Electronics Engineers (IEEE) Standards Coordinating Committee 21 (SCC21) “oversees the development of standards in the areas of fuel cells, photovoltaics (PV), dispersed generation, and energy storage and coordinates efforts in these fields among the various IEEE Societies and other affected organizations to ensure that all standards are consistent and properly reflect the views of all applicable disciplines.” [11] Under section 1254 of the USA Federal Energy Policy Act of 2005 IEEE Standard 1547 (Interconnecting Distributed Resources with Electric Power Systems) was born. The Act states “[i]nterconnection services shall be

offered based upon the standards developed by the Institute of Electrical and Electronics Engineers." [12] The 1547 series itself, offers standardized guidelines interconnecting distributed resources (DR) with electric power systems (EPS) addressing "performance, operation, testing, safety considerations, and maintenance of the interconnection." [13] Figure 8 describes the current progress for establishing the 1547 series.

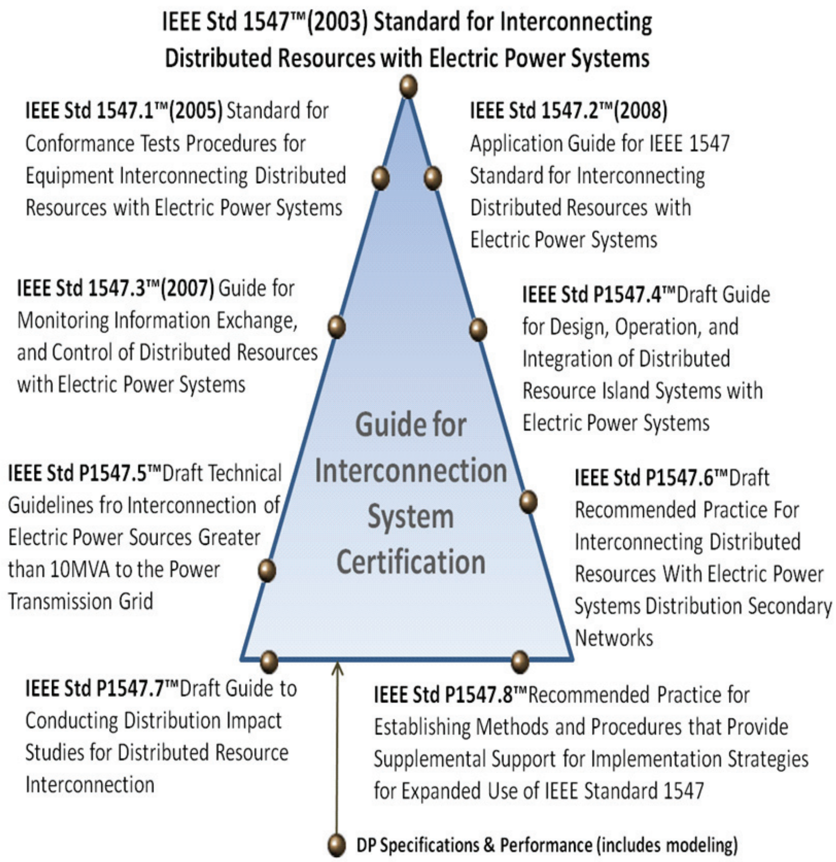


Figure 8. IEEE SCC21 1547 Series of Interconnection Standards [14]

An alternative to the microgrid technology is the Smart Grid. Smart Grids can be defined as "the integration of communications networks with the power grid in order to create an electricity-communications superhighway capable of monitoring its own health at all times, alerting operators immediately when problems arise and automatically taking corrective actions that enable the grid to fail gracefully and prevent a local failure from cascading out of control."

[15] More succinctly, the Energy Independence and Security Act of 2007 believes that Grid "refers to a distribution system that allows for flow of information from a customer's meter in two directions: both inside the house to thermostats, appliances, and other devices, and from the house back to the utility." [16]

Figure 9. Smart Grid Interoperability [17]

One key element in this infrastructure is the ability to maintain accurate time synchronization. This, in turn, allows the industry to draw distinct correlations amongst thousands, if not tens of thousands of events per day. This is so critical that the IEEE has developed IEEE 1588 a "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems." [18] This standard is meant to enable many disparate clocks to synch to one master clock, maintaining precision, resolution and stability while communicating on an Ethernet network or any other medium utilizing distributed communications. [19] The advent of the Smart Grid has also given rise to advanced RTUs and intelligent electronic devices (IEDs) that are capable of capturing and transferring a large amount

of data. These data transfers will require a more robust communications infrastructure. Smart Metering, a subset of Smart Grid technology, is used to provide "improved customer service, enhanced reliability, and lower outage management times." [20] These companies also hope to leverage this technology to establish "more efficient energy usage, reduced pollution, expanded use of renewable energy sources and improved security." [21] The federal stimulus bill has set aside $11 billion for Smart Grid initiatives, giving rise to 13 million smart meters at the end of 2009 and fueling plans for 50 million more. [21] This Advanced Metering Initiative (AMI) is also driven by the Energy Act of 2005. In particular, section 1252 addresses the concept and lays the standard for the establishment of smart metering. The Act establishes the type of time based rate schedules that can be implemented by the utility industry:

> (i) time-of-use pricing whereby electricity prices are set for a specific time period on an advance or forward basis, typically not changing more often than twice a year, based on the utility's cost of generating and/or purchasing such electricity at the wholesale level for the benefit of the consumer. Prices paid for energy consumed during these periods shall be pre-established and known to consumers in advance of such consumption, allowing them to vary their demand and usage in response to such prices and manage their energy costs by shifting usage to a lower cost period or reducing their consumption overall;
> (ii) critical peak pricing whereby time-of-use prices are in effect except for certain peak days, when prices may reflect the costs of generating and/or purchasing electricity at the wholesale level and when consumers may receive additional discounts for reducing peak period energy consumption;
> (iii) real-time pricing whereby electricity prices are set for a specific time period on an advanced or forward basis, reflecting the utility's cost of generating and/or purchasing electricity at the wholesale level, and may change as often as hourly; and
> (iv) credits for consumers with large loads who enter into pre-established peak load reduction agreements that reduce a utility's planned capacity obligations. [12]

AMI was implemented to meet these stringent guidelines. The meters utilize improvements in measuring energy usage, bi-directional communication and the capability to couple with the customers' home-area-network (HAN). This would allow the industry to directly monitor and /or control thermostats, appliances and other electrical devices. To date, this interface has not been implemented. [21] A visual representation is represented in Figure 10.

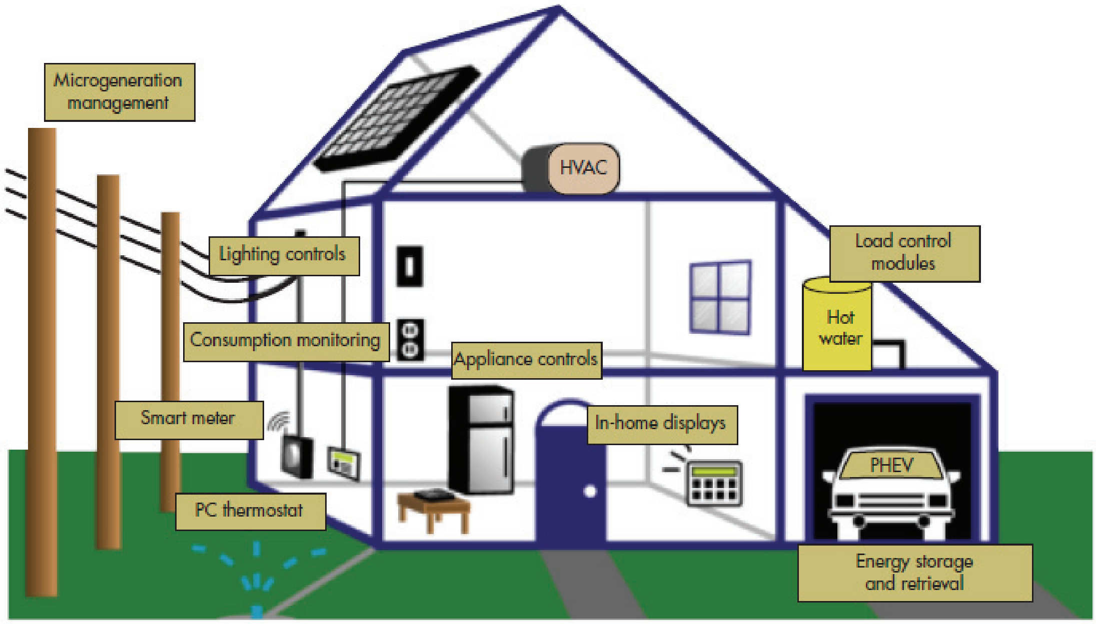


Figure 10. Smart Grid Integration [21]

Cyber Security

As Smart Grid technology becomes ubiquitous, concerns over integration with public and corporate communications infrastructure is a sobering reality. The utility industry has chosen to leverage the cost effective move away from isolated and expensive, proprietary networks and form close partnerships amongst public and corporate network infrastructures. Figure 11 depicts the ever-increasing locations of Advanced Metering Readings (AMRs), AMIs and Smart Grids.

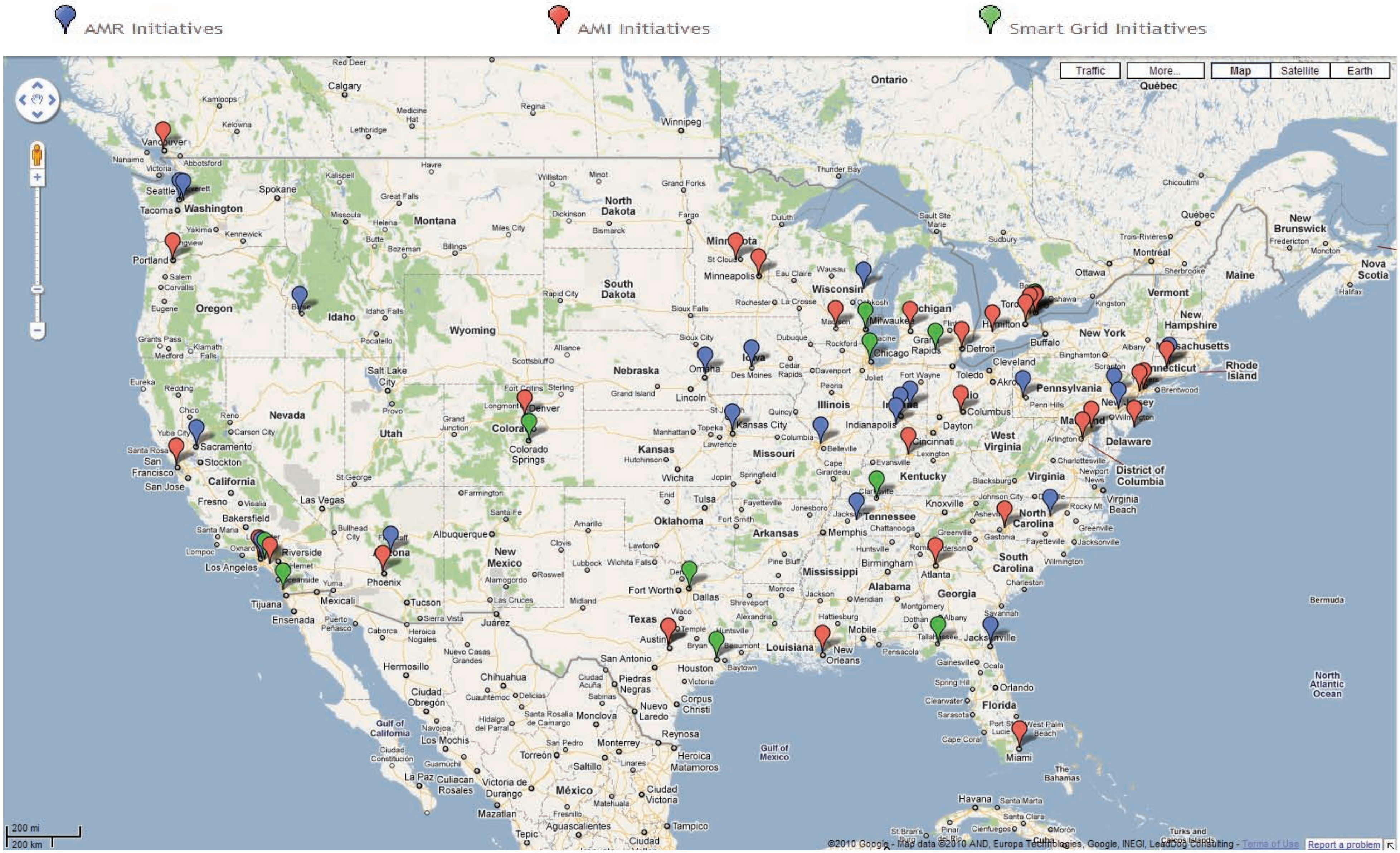


Figure 11. National Smart Grid Initiatives [22]

Unauthorized access to the electrical power grid (part of our nation's critical infrastructure) has been the focus of past administrations and frankly, remains a national security issue. President Clinton issued Presidential Decision Directive 63 (PDD-63). PDD-63's goal was "to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems." [23] Homeland Security Presidential Directive/HSPD-7 directs the office of the Secretary for Homeland Security to protect all information technology and telecommunications assets that are deemed critical to the national security of the United States. In March of 2009, President Obama directed the acting director of the National Cyber Security Division (NCSD) to complete a comprehensive Cyberspace Policy Review. Steps have been taken to study, act upon and provide guidance regarding cyber security for the power grid. Some have proposed and modeled security agents at the IED level (establishing security at the edges of the system) and at the PLC control layer where "more intelligent agents will utilize more complex rules for identification and detection of intrusive events and activities within the controllers." [24] In particular one entity has taken a lead role for proposing guidance and legislation for compliance by the industry. The North American Electric Reliability Corporation (NERC) "is an international, independent, self-regulatory, not-for-profit organization, whose mission is to ensure the reliability of the bulk power system in North America." [25] In 2006 and in compliance with the Energy Policy Act of 2005, the NERC petitioned and was certified by the Federal Energy Regulatory Commission (FERC) to become the "electric reliability organization" in the United States, however, [c]ompliance with approved NERC Reliability Standards didn't become mandatory and enforceable in the United States until 2007. [26]

System Security

There is a distinct difference between network security and electrical systems security. Network objectives range from data integrity, data confidentiality and data availability while electrical security tends to focus on human safety, maintaining normal operating conditions, and the protection of equipment and power lines. [24] A more succinct view of "system security involves practices designed to keep the system operating when components fail." [27] SCADA systems maintain security by actively monitoring the system, rapidly relaying the status of the power grid and taking the proper corrective action to maintain optimal power flows. Key to maintaining security is the ability to measure and react to a change in system state. This can be done by "studying the system with very fast algorithms, selecting only important cases for detailed analysis and using a computer system made up of multiple processors to gain speed." [27] There are a myriad of algorithms and formulas used to study and model electrical power flows. These methodologies are beyond the scope of this review. However, the ability to simulate and replicate these components is undeniably critical to maintaining the availability of this critical infrastructure.

Relevant Research

Simulators, Emulators and Physical Integration

The network simulators that are available for use in this environment are many and quite varied. They range from power system simulation/emulation to a federated suite of tools that allow us to readily clone a realistic system. Let's discuss the difference between simulation, emulation and physical integration. Simulation "means that the computer assisted simulation technologies are being applied in…networking algorithms or systems by using software engineering." [28] In essence, a simulation is software driven thus lending to easy setup and use,

but a much greater degree of abstraction. Emulation/virtualization "uses machine-code translation to implement "machine within a machine" functionality." [29] Lastly, physical implementation is simply integration of the physical/real device with the simulated environment. This can be done in one of two ways – via a network interface card into the simulated environment or through an emulated interface.

A few things come to mind when choosing a viable simulator/emulator. First and foremost is documentation. In some cases, the developer is left to her own wiles without adequate documentation and timely technical support. Building your simulation environment can be difficult, especially since power system simulation can encompass a slew of protocols. High speed and low speed power line technology (PLC), IEEE 802.15.4, cellular networks and WiMax are just a few of the standards that can be utilized in Smart Grid communications. [30] In addition, IP protocols are numerous and varied; consisting of TCP, UDP, HTTP, TELNET, FTP, TFTP, SNMP and DHCP.[30]

Next, would be realism. How close to reality are the actual simulations? This is where critical analysis of the software comes into play. Many of the parameters that drive this realism are very complicated algorithms and subroutines. One critical point of focus is maintaining synchronization with a real-time clock. The most common method used in popular tools today is the trapezoidal integration method. $x_t = \frac{\Delta t}{2} f_t + \frac{\Delta t}{2} f_{t-\Delta t} + x_{t-\Delta t}$. [31] "The terms found at t - Δt constitute history terms and all quantities at time-point t are also related through network equations. The integration time-step Δt can be fixed or variable." [31]. It must be noted that as the size of the network increases, the variable time-step leads to significantly higher computational overhead. However, using a fixed-time step simulation isn't without its own drawbacks. When used with cyclically switching circuits, it often leads to the emergence of

jitter. This anomaly was overcome in a simulation of a single-phase thyristor converter by using the ARTEMIS™-RTE algorithm. The "algorithm is an interpolation-extrapolation algorithm. When a switching discontinuity is detected, states are interpolated for the fraction of the step detected. After the discontinuity has been interpolated, a normal iteration is made, followed by an extrapolation to resynchronize the simulation with the fixed time-step frame." [32]

Cost is also a very critical limiting factor. Some of these tools are inordinately expensive. Proprietary simulation engines (the good ones) require a substantial investment up front. This investment drives the appropriate research and development, documentation and technical support that is often very critical for the novice. And, finally, ease of use should be a serious consideration. If the tool has a steep learning curve then it's going to take more time to develop your simulations.

Network Simulators

During the review, the author encountered three main network simulators. Each had its pros and cons. The first was NS-2 or Network Simulator 2. NS-2 is a very powerful simulation tool that was developed by the University of California, Berkeley. It is an object-oriented, discrete event driven simulator that is based on C++ as the programming language and OTcl as the scripting language. The "script is used to initiate the event scheduler, set up the network topology, and tell [the] traffic source when to start and stop sending packets through [the] event scheduler." [28] The issue with NS-2 is documentation and support. Although the modules are robust, they have been developed by individuals that provide little to no documentation and they no longer have the time nor the will to provide anything but rudimentary support.

Network Simulator 3 (NS-3) is the follow on to NS-2 but it is not backwards compatible. It is also compiled in C++; however, it uses Python as its scripting engine. Portability of NS-2 modules to NS-3 is ongoing. Furthermore, the developers list the following new capabilities: "handling multiple interfaces on nodes correctly, use of IP addressing and more alignment with Internet protocols and designs, more detailed 802.11 models, etc." [33] NS-3 also has the ability to be traced with Wireshark™ and other tools via the .pcap libraries. Unlike NS-2, documentation is detailed and robust. Supporting documentation can also be found in Blogs, Mailing Lists, Bug Trackers, etc.

The last simulation/emulation tool reviewed was OPNET® Modeler®. Of the three, OPNET® was the only tool that is not free. Hence, the documentation and support is above and beyond what is to be expected for a non-commercial product. The drawback with any commercial entity is the source code is not available to the public and any enhancements need to be developed by the OPNET® Corporation. Any modification to the source is relatively difficult and not supported. OPNET® is a mature and very popular suite of tools that model, simulate and analyze a myriad of networks topologies. In a study of Substation Automation Systems (SAS) OPNET® is used to model the implementation of IEC 61850 via IEDs. "The proposed OPNET® models, aim to simulate the various SAS network under different scenarios, allowing the user to set the raw sample rate, fault time, number of faults, background traffic and other configuration parameters." [34] The author's configuration follows in Figure 12.

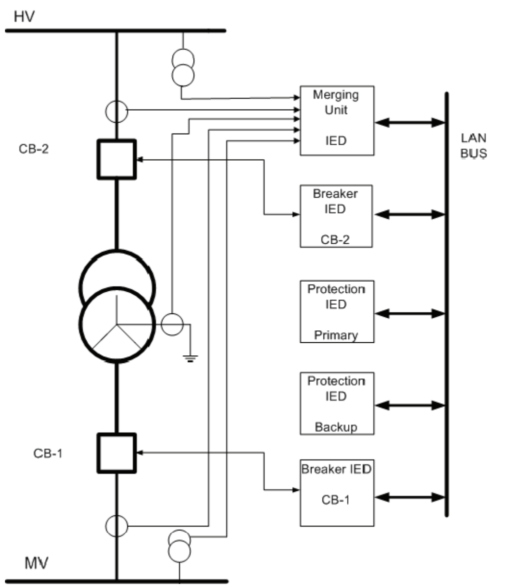


Figure 12. 69Kv Substation Single Line Diagram [34]

Breaker IED
1. Controls breaker circuit
2. Monitors state and condition of breaker
3. Receives trip/close command from protection IEDs or HMI and sends state change through bus

Protection/Control IED
1. Integrates substation protection and control functions
2. Priority tagging disabled

Merging Unit IED
1. Merges three phase current and voltage
2. Transmits raw data sampled values to the LAN

Data
1. Packaged in Ethernet Packet
2. Sent via multicast messages
3. Configured options
   a. Sample rate
   b. Start and stop time
   c. Packet size
   d. Address and multicast group address
   e. Transmission type (P2P, multicast, broadcast

4. Background traffic simulated by attached workstations

OPNET® Modeler® has a node and process model editor that assists with configuration and design. Figure 13 is the node representation for the Merging Unit, Breaker and Protection IEDs.

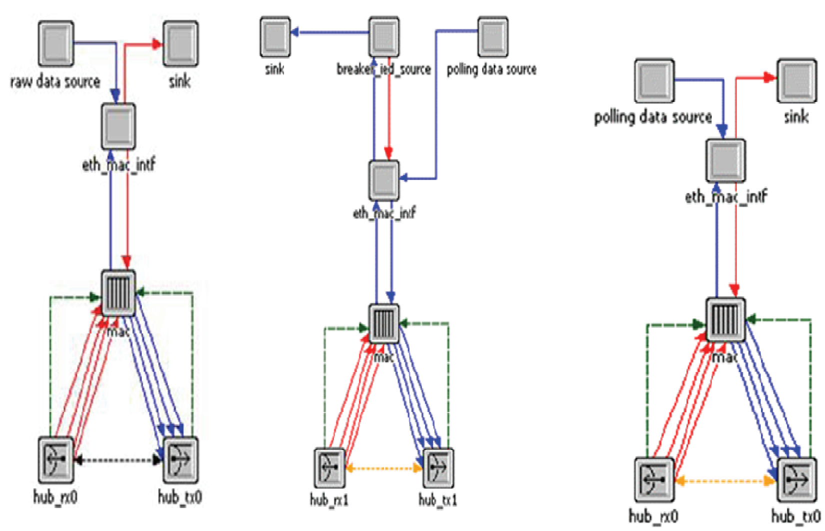


Figure 13. Merging Unit IED, Breaker IED and Protection IED (from left to right) [34]

OPNET® generated transfer time delay graph

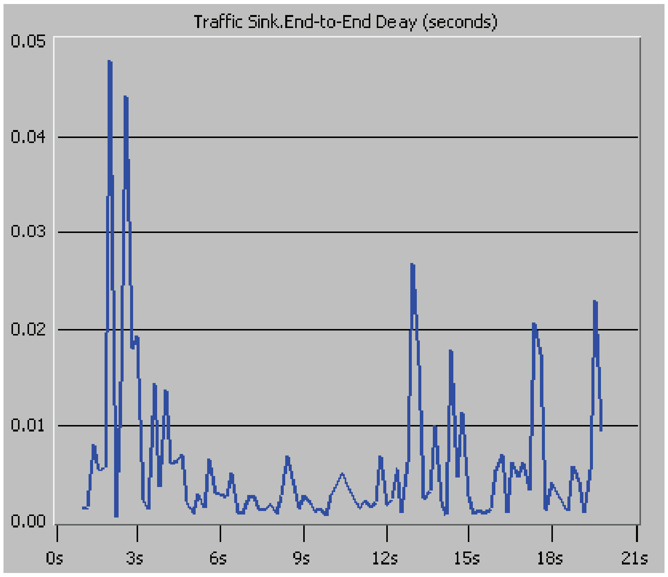


Figure 14. End to End delay diagram [34]

With the results in figure 14, the authors were able to conclude that the use of OPNET® to model a SAS is an effective tool. Engineers and researchers alike can use OPNET® to design and forecast the network load for current and future systems.

Of particular importance in the OPNET® suite of tools is the System-in-the-loop (SITL) module. This module allows the creator of the simulation environment to easily utilize physical hardware in the simulation. One can incorporate servers, workstations, switches, routers, etc. in the model being simulated. This is very important and will be covered during our discussion of Simulated, Emulated, and Physical Investigative Analysis (SEPIA).

Power System Simulation

The only power system simulator reviewed was HVDC Manitoba's Power Systems Computer Aided Design/Electromagnetic Transients including DC (PSCAD/EMTDC) Engine. PSCAD is the graphical interface while "EMTDC is a powerful simulation engine that has been evolving since the mid-1970s." [35] A detailed understanding of power algorithms and design is needed to adequately leverage the power of PSCAD. Since this tool is designed for use within

the industry, without that knowledge there is a rather steep learning curve, especially, if you need to modify any of the simulation algorithms. "EMTDC results are solved as instantaneous values in time, yet can be converted into phasor magnitudes and angles via built-in transducer and measurement functions in PSCAD - similar to the way real system measurements are performed." [35] In addition, this tool is also based on the fixed time-step trapezoidal integration method discussed in the previous section and can be utilized in an offline, hybrid or real time simulation mode. [31] The compiler for the EMTDC engine is FORTRAN. The preferred version is FORTRAN 95 but with minor modifications it is backwards compatible to the earlier versions. The main program structure consists of the System Dynamics Section (DSDYN), the Electric Network Solution and the output definition subroutine (DSOUT). Flexibility is maintained by allowing the user to access most EMTDC features in the DSDYN and DSOUT sections. Detailed benefits from the use of PSCAD are many and varied, however, any additional specifics based on these techniques were well beyond the scope of this review.

Simulated, Emulated, and Physical Investigative Analysis (SEPIA) of Networked Systems

Sandia National Laboratory's "SEPIA environments enable an analyst to rapidly configure hybrid environments to pass network traffic and perform, from the outside, like real networks. This provides higher fidelity representations of key network nodes while still leveraging the scalability and cost advantages of simulation tools." [29] It is believed that this environment facilitates the investigation and protection techniques that are not readily available via a non-hybrid solution. In today's simulation environment the simulator has four choices. The first is to develop an environment that is strictly simulated in nature. While doing so is relatively inexpensive (depending on the suite of tools used) the fidelity of such an approach fails

to answer all the hard questions; one being, the accurate representation of specific threats and/or vulnerabilities to scale. Another drawback is the fact that "implementation codes often get refined and features get added without being simulated and hence the simulation models and implementations [differ] in capability." [29] This leads to the study of the implementation itself, which, since it's not to scale, does not reveal true fidelity. Now, researchers and vendors have taken advantage of the latest ability to emulate/virtualize large networks (second choice). The scale of these networks is only limited by the available resource and far outweighs the expense of building and testing on live networks (third choice). SEPIA uses OPNET®'s SITL tools by:

1. It extended upon OPNET®'s SITL tools for allowing real traffic to pass through the simulated networks, by developing new techniques that allow complex real and emulated systems to interoperate with their simulated counterparts.

2. It extended upon existing emulators by developing hypervisors that allows researchers to launch and manage connected networks of emulated network devices from a single application.

3. It developed a new understanding of how the simulations models within these SEPIA environments will scale.

4. It developed tools to automatically configure SEPIA testbeds for rapid implementation. [29]

In the end, the best scenario is the fourth and final choice. A true hybrid environment that consists of a SEPIA environment and is, in essence, an amalgam of all three of the previous choices: simulation, emulation and physical representations of a "real" network. In Figure 15, remote clients are able to access the experimental environment through a Virtual Private Network (VPN) and gain access to the physical/virtual hosts.

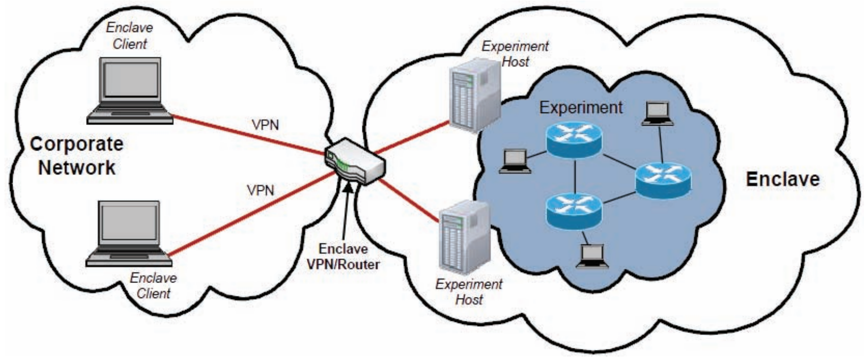


Figure 15. Testbed Topology [29]

The final environment encapsulates simulated, emulated and real devices.

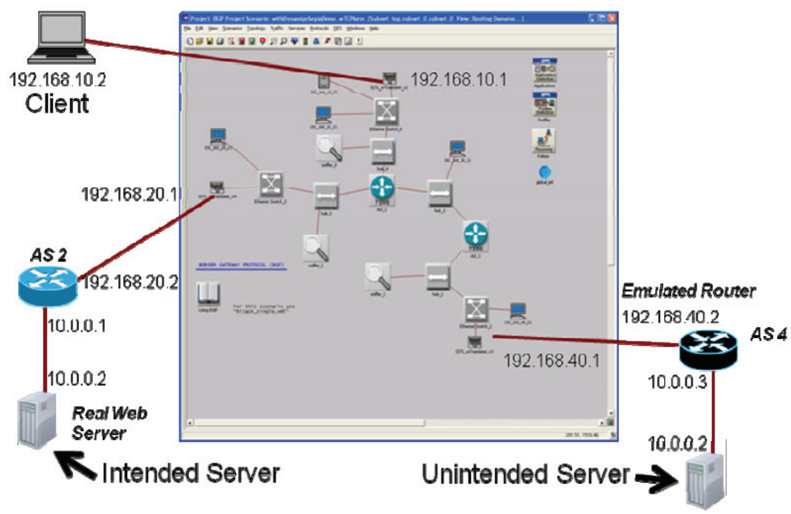


Figure 16. Demo network [29]

Federated Environments

The Electric Power and Communication Synchronizing Simulator (EPOCHS)

The first federated system evaluated was EPOCHS. "EPOCHS is a distributed simulation platform that links commercial and high quality simulators through the use of a runtime infrastructure (RTI) to allow modelers to investigate electric power scenarios that involve network communication. EPOCHS seamlessly links simulation systems from a modeler's perspective, enabling them to investigate power protection and control scenarios that

combine communication with the ability to sense the state of a power system and to react to it in real-time." [36] In particular, this particular version federated PSCAD/EMTDC, NS2 and AgentHQ. EPOCHS is built upon an RTI compiled in C++. This RTI communicates with AgentHQ, NS2 and PSCAD/EMTDC via a Tool Command Language (TCL) script. After synchronization of PSCAD and NS-2 the RTI yields control to the agents. There are three different agents in the simulation. The agents communicate with IEDs and/or each other. There is a primary agent, backup agent and load agent. "Primary agents are responsible for first zone protection, covering 100% of the transmission line. Backup agents are responsible for the third zone protection, which covers the first zone plus all the transmission lines connected to the remote end of the first zone. Load agents are only responsible for sending their current state (usually their current phasors) to the backup agents." [36] The agents then receive/send updates of all pertinent variables (calculated and measured) in NS-2 and PSCAD. The rules for their behavior are listed in Table 4.

After completion of one time-step of 2 milliseconds the agent then relinquishes control back to the RTI. The RTI now notifies NS-2 and PSCAD that a time -step was completed and both engines advance by another 2 milliseconds. At this time the RTI will pass messages to the agents, where they are queued until they, again, are granted control. [36]. The benefits of this model are twofold. First, one is able to affectively study the communication between the agents and monitor/measure traversal times between nodes in a simulation environment that varies per availability of the inter-nodal communication links. Second, "[d]istribution, intelligence, communication, and autonomy make the intelligent agents appear as a suitable framework for realizing the evolution to the smart grid." [37]

The goal of this research was to capitalize on the dynamic capability of EPOCHS while at the same time migrating from a poorly supported network simulator. NS2 has strong roots in the academic environment, making it quite flexible, but very code intensive. The use of OPNET® allows the user to capitalize on the extensive commercial support, graphical user interface and tools, and innovative statistical analysis package. Additionally, this proof of concepts lays the groundwork for further analysis with tools common in industry, establishing a methodology that the utilities community can use to study and model more complex and sophisticated power topologies.

Table 4. Rules for Primary and Backup Agent Behavior [36]

Rule	IF	THEN
	Electrical Event	
	Primary Agent	
1	Primary_Differential_Current > Limit	- Fault_Status = Detected - Send INTERTRIP to correspondent primary agent - Start trip_timer
2	Local_Current still present after 50 ms of fault occurrence (breaker_timer > 50 ms)	- Breaker_Failure = Detected - Send NEIGHBOUR_TRIP to the primary agents located at the same bus
	Backup Agent	
3	Backup_Differential_Current > Limit	- Fault_Status = Detected - Send BACKUP_TRIP to correpondent primary agents - Start backup_timer
4	Local_Current still present after 100 ms of fault occurrence (backup_timer > 100)	- Open breaker (FORCED_TRIP)
	Communication Event	
	Primary Agent	
5	No message arrives within 15 ms of fault detection (trip_timer > 15 ms)	- Open breaker (FORCED_TRIP) - Check for breaker failure → Start breaker_timer
6	Receives INTERTRIP or BACKUP_TRIP and FAULT_STATUS = Detected	- Open breaker
7	Receives INTERTRIP and BACKUP_TRIP	- Open breaker
8	Receives INTERTRIP_RESPONSE = Negative	- Disable trip_timer and wait for BACKUP_TRIP
9	Receives NEIGHBOUR_TRIP and BACKUP_TRIP	- Open breaker

Virtual Control System Environment (VCSE)

VCSE is best described as a suite of modeling components that uses SEPIA for high fidelity, broad-reaching analyses. [38] The main thrust behind the development of VCSE is the ability to use a suite of tools to study and evaluate cyber security methodologies in a SCADA environment. Not many tools are capable of federating all the components needed to make this analysis a reality. The paper's literary review lists three possible alternatives:

- Real-time Immersive Network Simulation Environment for Network Security Exercises (RINSE)
    - Is a tool for realistic emulation of large networks as well as network transactions, attacks, and defenses
    - Has unique capabilities, which make it suitable for cyber security and game-playing exercises including large-scale real-time human/machine-in-the-loop network simulation support, multi-resolution network traffic models, and novel routing simulation techniques
- The Real Time Digital Simulator (RTDS)
    - Provides power systems simulation technology for fast, reliable, accurate, and cost effective study of power systems with complex High Voltage Alternating Current (HVAC) and High Voltage Direct Current (HVDC) networks
    - Simulator is a fully digital electromagnetic transients power system simulator that operates in real time
- Critical Infrastructure Protection and Resiliency Simulator (CIPR/sim)
    - In cooperation with the Department of Defense, scientists and engineers at Idaho National Laboratory have developed an advanced simulation

technology called CIPR/sim which allows emergency planners to visualize the real-time cascading effects of multiple infrastructure failures before an actual emergency occurs

  - Responders are better prepared and more responsive and accurate when analyzing critical incident data [38]

Sandia chose to develop VCSE because they believe it addresses the following needs:

- Reduce energy system exposure to harm, cyber attacks, and accidents
- Uncover system vulnerabilities that stem from unencrypted, unsecured data on IP routed computer networks
- Develop, test, and validate counter measures to prevent system damage and safeguard energy networks
- Prevent disruptions [38]

The extent of VCSE's capabilities is not all encompassing. In particular, the level of abstraction is meant to be controlled in order to provide the right amount of fidelity on the critical area. Providing a complete fidelity environment would use a tremendous amount of resources and, in the end, would be counterproductive. It is through this limited scope, the focus on areas of interest, that it is then possible to integrate a SEPIA environment. In addition, the developers of VCSE strive to fulfill the following four objectives.

1. Create a simulation framework
2. Develop simulation-configuration user interfaces
3. Develop simulation-execution user interfaces
4. Develop or employ analysis tools. [38]

Using this framework, VCSE is able to successfully simulate the SCADA systems by interfacing with real and simulated remote terminal units (RTUs), human machine interfaces (HMIs) and various networking components (real, simulated and emulated).

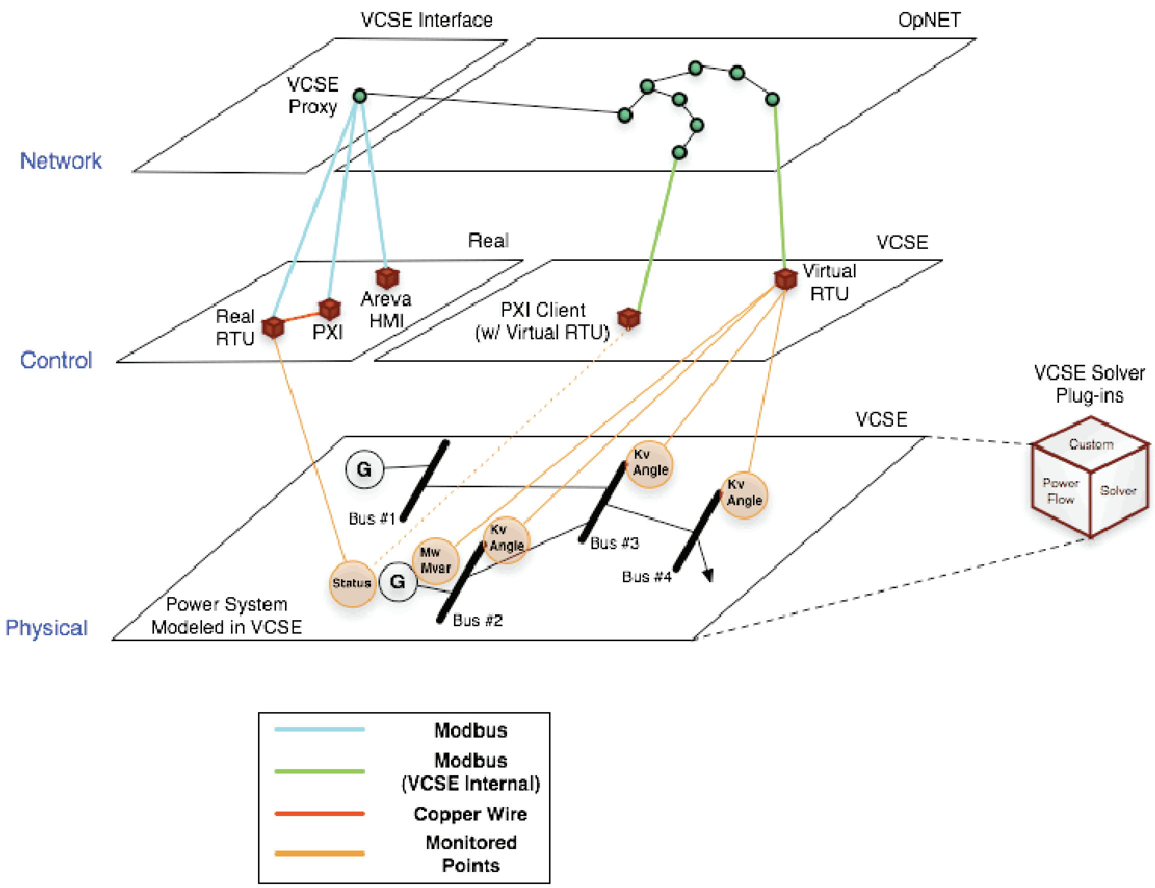


Figure 17. VCSE model [38]

The following components were integrated into the VCSE suite:

- Infrastructure Models
    - A Sandia-developed Newton–Raphson Steady State Power Simulator
    - University of Missouri (UMR)-developed Dynamic Power Simulator
    - PowerWorld© [14] Steady State Power Simulator
- Network Components

    - OPNET® [15] Network Simulator
    - Network-In-a-Box (NIB) Network Simulator [16]
    - Real Network Devices (routers, switches, etc.)
- Control-System Interfaces
    - RTU simulation models with ModBus [17] interfaces
    - Telvent SAGE 1330 RTU using a National Instruments (NI) PXI-1042 with NI PXI-8196 digital to analog converter to connect to VCSE
- Human Machine Interfaces (HMIs)
    - Areva E-TERRACONTROL based operator's consol (HMI) [18]
    - A Sandia-developed Web-based HMI
- Cyber Security Components
    - An Open Process control system Security Architecture for Interoperable Design (OPSAID) prototype security device [38]

These components were critical to executing the SEPIA environment; however, simulation models are developed using VCSE-SF. VCSE-SF "integrates disparate modeling and simulation capabilities across the VCSE-SF boundary through a software plug-in architecture. In addition, it can interface with external models through VCSE-SF-based network proxy interface modules (a.k.a., class instances)." [38] VCSE-SF supports modeling and the integration of code that incorporates SEPIA functionality. Of particular note is the ability of VCSE-SF to provide a dynamic environment for intelligent electronic devices (core components of a SCADA system). Sandia was able to create a simulated environment that modeled a city with the approximate size of San Diego, a 24-bus power system with 11 generators and 17 loads. Currently it is unclear if this was strictly a simulated or a true SEPIA environment. One additional scenario used a

dynamic power simulator to reproduce a 5 generator/14 bus system. Sandia proved (successfully simulated) that by disabling the load of one of the generators the control systems of the remaining generators were forced to respond.

As stated previously, one of the goals of this study is to create a hybrid power and network simulator that is both dynamic and has the flexibility to model any and all grid topologies. VCSE has primarily been used within a static power environment, lacking the capability to work with transient power solvers that model interactions on a realistic scale. This work seeks to lay the foundation for the incorporation of transient power flows, allowing the industry to accurately model and solve realistic power anomalies, successfully bridging the gap between EPOCHS and VCSE.

Summary

In conclusion, the evolution of the electric power grid has come a long way. Through deregulation, the electric utility industry has partnered with the federal government to maintain security of the grid. Old protocols have been replaced with new robust communication constructs that guarantee that we can take advantage of modern communication networks. It is only through modernization that new distributed Smart Grid and microgrid networks allow electric utility customers to cut the demand for an ever increasing appetite for energy. However, in order to continue these efforts those developing and researching new methodologies must have the correct tools. These tools should provide a realistic environment that measures all factors, allowing those planning future energy distribution infrastructure to make efficient, cost effective choices, reducing overall cost, consumption and taking advantage of all that modern and breakthrough technologies have to offer.

III. Methodology

Chapter Overview

The purpose of this chapter is to lay out the methodology for federating (or combining) a dynamic power simulation environment. This environment is made up of several stand-alone programs. First, OPNET® is used to simulate the networking protocols and perform the traffic analysis. Next, PowerWorld© is used to simulate the electrical components absent transient communication. Furthermore, a simulation manager will be used to manage interaction between, both, the power and network simulators. Aditionally, a model of the Electric Power and Communication Synchronizing Simulator (EPOCHS) agents will be used to supervise and control the simulation. These agents will coexist within the communication environment and facilitate the transfer of information between the different nodes/buses within previously defined end-to-end delay constraints. OPNET's statistical analysis tool will be used to measure, quantify and justify these final measurements. Finally, a brief overview of the experiments and parameters that will be measured after successful federation of the disparate simulation engines will be discussed.

This chapter has several goals. The first is to describe the electrical simulation environment and the creation of the model in PowerWorld©. Next, will be a corresponding description of the communications infrastructure in OPNET®. Third is the creation of the federated environment between OPNET® and PowerWorld©. And last, is the creation of the agents and their interaction with the entire system.

Further expansion of current Smart Grid and micro-grid technology warrants the development of a sound test environment and protocols. Utility companies cannot afford to arbitrarily add to the burden of their communication networks without taking the appropriate

steps to ensure they have taken all necessary measures guaranteeing the viability of their networks. Although there are existing federated power/communication environments that have the capability to scale and satisfy this need, none is able to do this without the interaction of agents that facilitate the ability to ensure sound communications throughout the network. Not only can agent technology solidify sound communications but it also ensures that the appropriate measures are taken to avoid power system failure, utilizing new and existing algorithms to quickly react to transient effects. In addition, though beyond the scope of this paper, agents can implement trust systems that enhance the security of the power grid. With modern utility companies looking to leverage and take advantage of the additional bandwidth gained by expanding existing power grid infrastructure, this action, mandated by the implementation of Smart Grid and micro-grid advancement, closely marries aforementioned proprietary networks with Internet infrastructure. This close association with unsecured networks exposes expanding power grid infrastructure to all of the existing security vulnerabilities that affect the Internet. By implementing existing simulation technology with an agent environment, utility companies will be able to affectively model their expanding networks, while at the same time, deploying, simulating and planning agent interaction throughout their network.

Test Subjects

The initial power system was based on the IEEE 14 Bus Power Flow Test Case found on the University of Washington's research site [39]. This test case was chosen because the lack of complexity makes it simple to test basic concepts and it was also the test case that was used by the team that developed the EPOCHS, of which my logical algorithm is based. The standard oneline or pictorial representation is detailed in Figure 18. Next, a highly complex IEEE 145 Bus Power Flow Test Case was modeled and tested against the same overall constraints. This

test case was chosen to illustrate the ability of this simulator to scale to realistic models while, simultaneously, preserving the bounds of pre-established constraints.

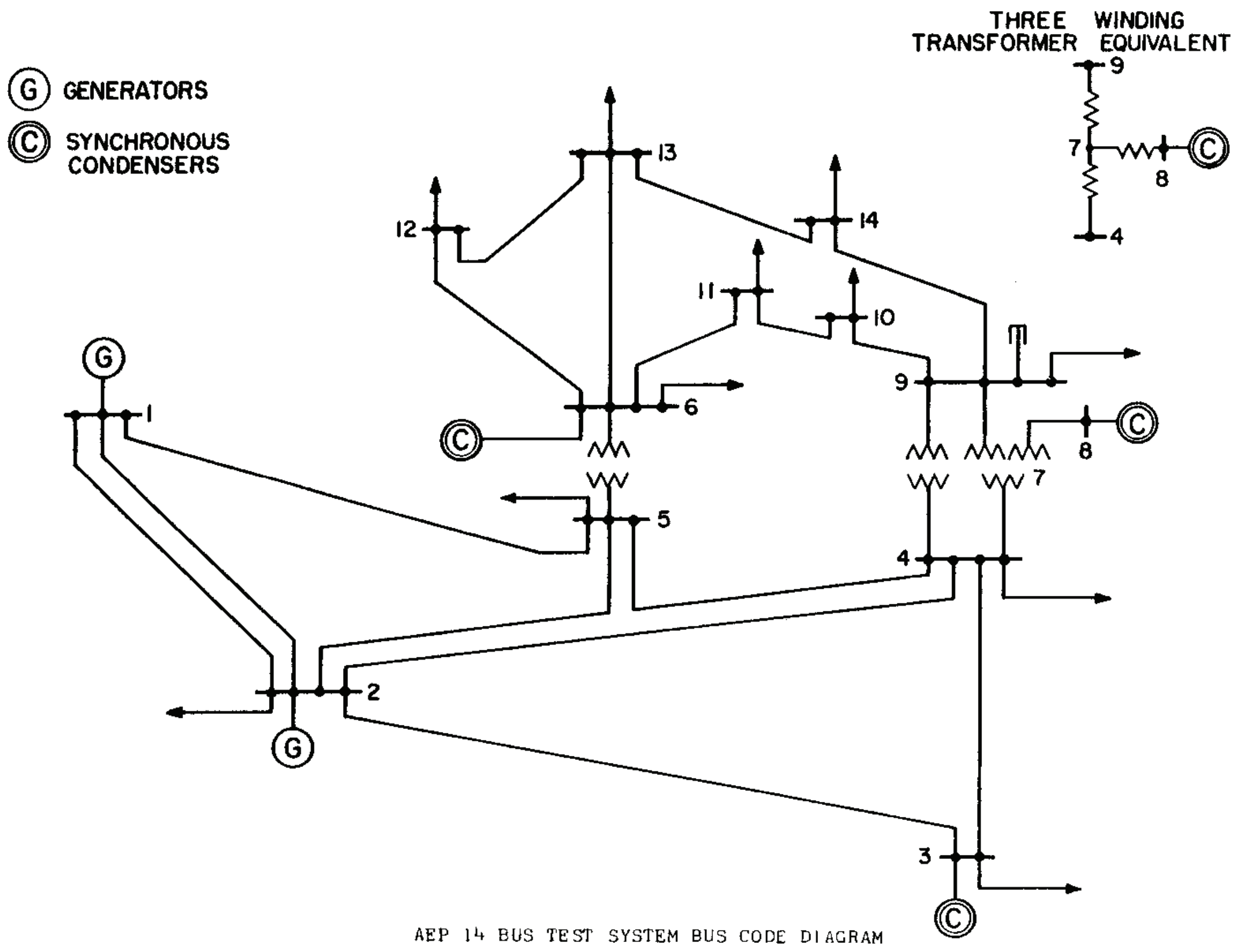


Figure 18. 14 Bus one line diagram[40]

An equivalent schematic (Figure 19) was produced by Hopkinson, et-al in a paper based on the implementation of EPOCHS.

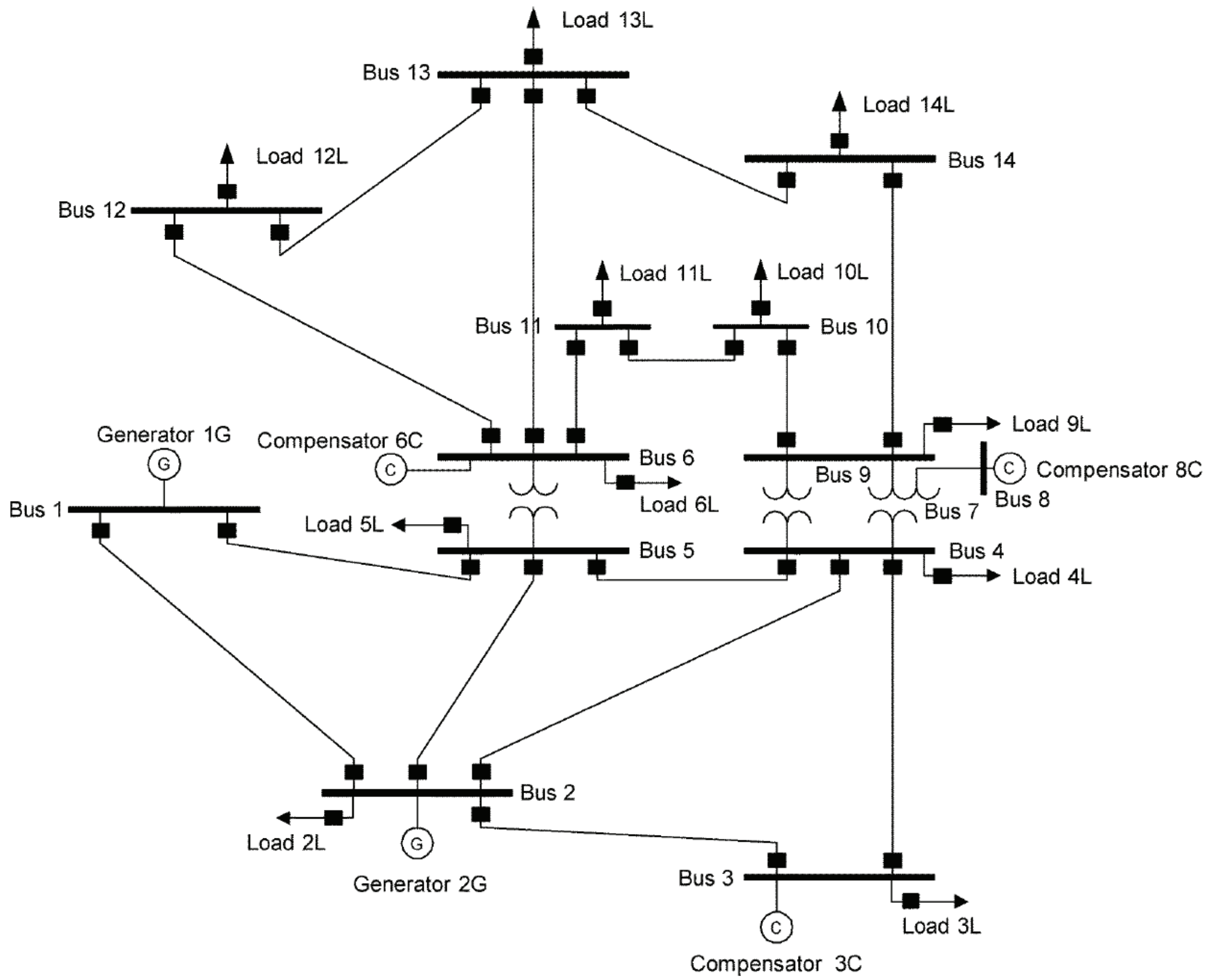


Figure 19. IEEE 14-bus system [41]

The authors continue to say "[a]ll transmission lines were modeled based on the PI [power information] model of the line, and all sources were modeled as constant power sources." [41] In essence, nodes that only housed transformers were assumed to be located at the same substation and were not given their own transmission line. This very same implementation will be modeled in PowerWorld© using the native oneline tool. A visual representation of the completed schematic follows in Figure 20….

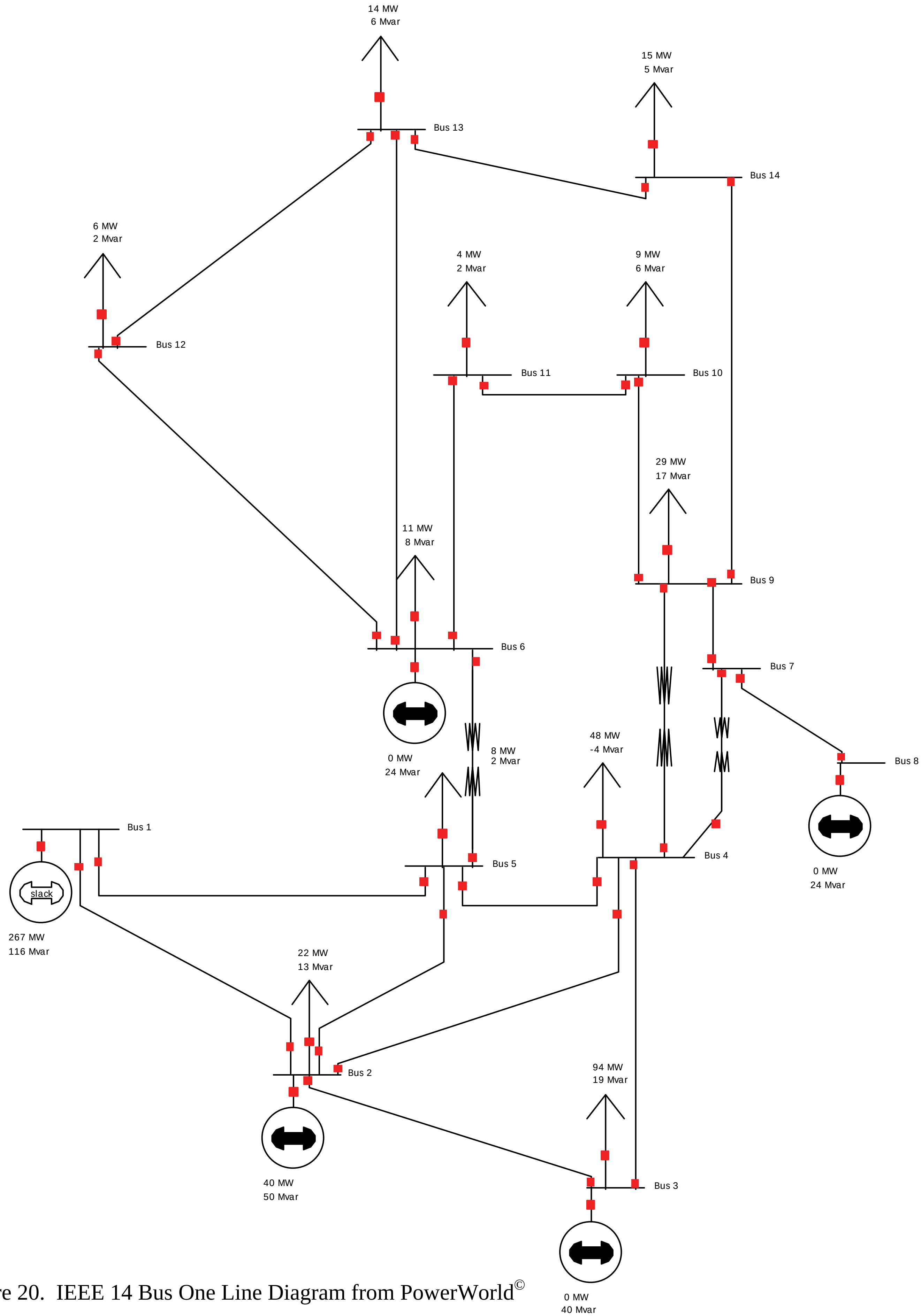


Figure 20. IEEE 14 Bus One Line Diagram from PowerWorld©

It's then, simply a matter of using the PowerWorld© import tool to bring in the associated power settings for the power components (minus topographical data) from the common data format file. This allows PowerWorld© to accurately simulate the interactions of the power environment. As stated before, this case does not have any transient capability, but it will be used as the benchmark that models the initial interaction between the federated environments. The communication links were modeled running parallel to existing transmission lines and, as stated in the previous paragraph, substations were allocated one communication node. Looking at the model in Figure 21, buses five and six were consolidated at node five and buses four, seven, eight and nine reside at node four.

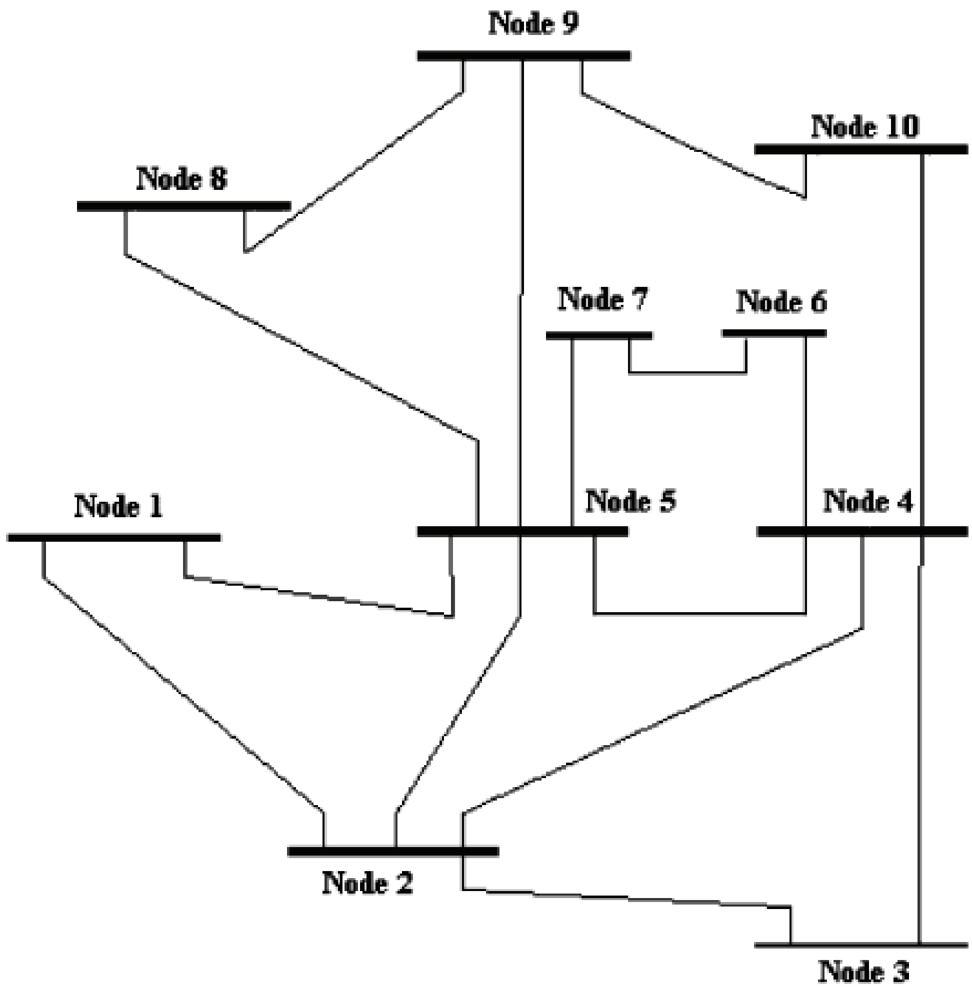


Figure 21. Communication Layout [41]

Long haul links consisting of data rates equaling 1.544 Mbps (T1), or 44.736 Mbps (T3) were established between respective communication nodes. This data rate was chosen in order to mimic the most effective long haul links in the industry. Cisco © 7204 switches were chosen to route IP traffic throughout the network. These routers had the appropriate number of serial ports needed to establish the long haul links. The logical representation is presented in Figure 22.

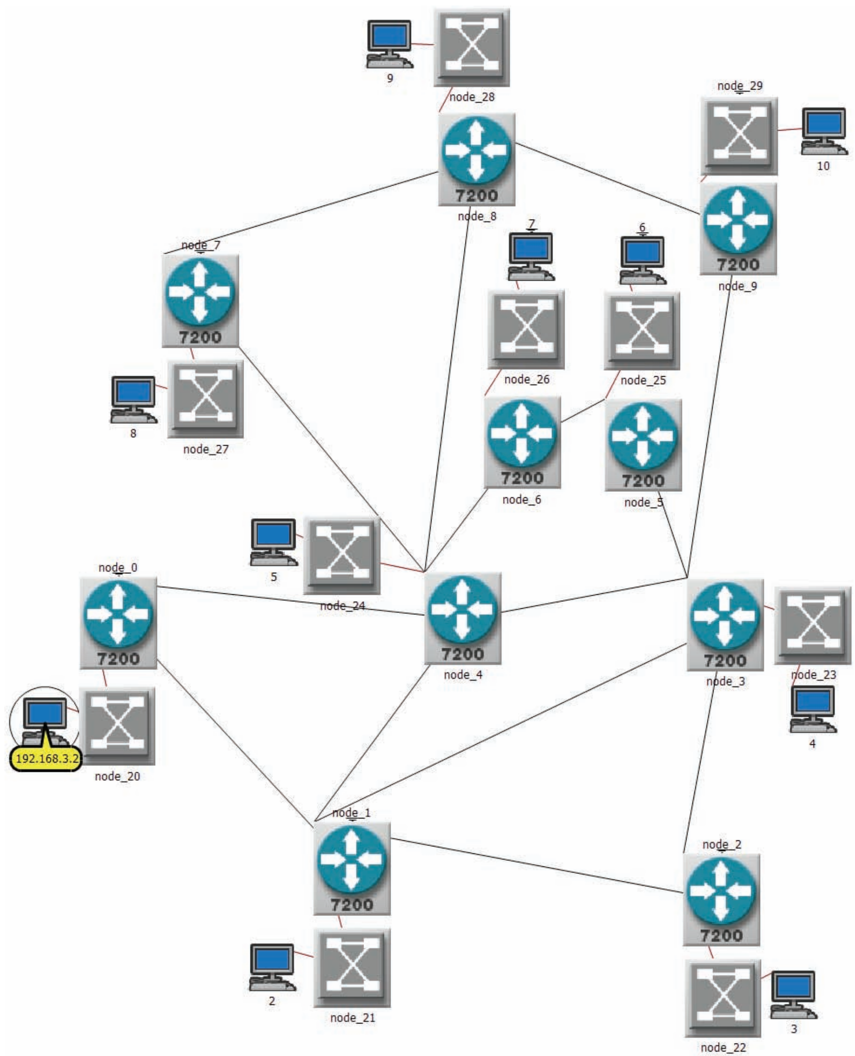


Figure 22. OPNET® IEEE 14 bus long haul links

All LAN links are defined as full duplex 100Mbps with the goal of keeping end-to-end delay below 2ms. Background traffic on all communication lines (LAN and long haul) were generated to mimic a prototypical LAN. In order to investigate whether agent interaction is viable, the simulated network will also carry traffic representing/modeling prototypical DNP3 communication alongside the aforementioned LAN traffic. LAN traffic and power traffic were generated by gathering data dumps from their respective networks. Data was processed in 30 second, 60 second and when relevant, 60 minute intervals (Tables 5 – 14). These intervals were then modeled using the OPNET® traffic information attribute for all links. Communication

between nodes was implemented with background traffic (displayed in the following tables) categorized as heavy and light loads. These loads were modeled at the macro level. Specifically, all packet sizes were given a value based on the aggregate averages of all of the packets captured/analyzed during the chosen snapshot. Subsequently, data rates for background traffic were given a constant average as well. Depending on the percentage of the total load placed on the links, whether it is 100% or 150%, these packet sizes and data rates had an inverse relationship with available bandwidth. For instance, if one chose to increase the background traffic from 100% to 125%, the remaining bandwidth available to additional traffic, say agent interaction, would decrease by 25%.

Table 5. Snapshot - light internal LAN traffic

Lightest_Internal_0000							
	Packets	Time (sec)	Avg. Packets/sec	Avg. Packet size (bytes)	Bytes	Avg. bytes/sec	Avg. Mbit/sec
Total	1123375	60	18722.994	466.687	524264154	8737748.573	69.902

Table 6. Snapshot - heavy internal LAN traffic

Heaviest_Internal_00005							
	Packets	Time (sec)	Avg. Packets/sec	Avg. Packet size (bytes)	Bytes	Avg. bytes/sec	Avg. Mbit/sec
30_00	1124220	30	37474.042	726.504	816750185	27225036.891	217.8
30_01	970774	30	32359.252	676.902	657118929	21904044.724	175.232
Total	2094994	60	34916.647	701.703	1473869114	24564540.808	196.516

Table 7. Snapshot - light external LAN traffic

Lightest_External_00018							
	Packets	Time (sec)	Avg. Packets/sec	Avg. Packet size (bytes)	Bytes	Avg. bytes/sec	Avg. Mbit/sec
Total	166637	60	2777.318	621.35	103539900	1725686.827	13.805

Table 8. Snapshot - heavy external LAN traffic

Heaviest_External_00008							
	Packets	Time (sec)	Avg. Packets/sec	Avg. Packet size (bytes)	Bytes	Avg. bytes/sec	Avg. Mbit/sec
Total	345891	60	5764.92	789.583	273109657	4551882.766	36.415

Table 9. Snapshot - heavy Internal SCADA

	Packets	Time	Avg. Packets/sec	Avg. Packet size (bytes)	Bytes	Avg. bytes/sec	Avg. Mbit/sec	% of total Traffic
Total	1984649	3599.959	551.298	538.717	1069163277	296993.205	2.376	
DNP3	17384	3599.765	4.829	84.994	1477534	410.453	0.003	0.88%
SMB	59105	3595.672	16.438	127.6	7541805	2097.467	0.017	2.98%
MBTCP	17986	3599.54	4.997	80.498	1447844	402.23	0.003	0.91%
TCP (only)	1889609	3599.959	524.897	560.252	1058656998	294074.761	20353	95.21%
UDP	320	3113.458	0.103	192.684	61659	19.804	0	0.02%
ARP	442	3303.601	0.134	62.118	27456	8.311	0	0.02%

Table 10. Snapshot - light internal SCADA

	Packets	Time	Avg. Packets/sec	Avg. Packet size (bytes)	Bytes	Avg. bytes/sec	Avg. Mbit/sec	% of total Traffic
Total	890743	3599.845	247.439	116.103	103417791	28728.398	0.23	
DNP3	17910	3598.608	4.977	85.004	1522424	423.059	0.003	2.01%
SMB	57216	3593.369	15.923	128.049	7326446	2038.88	0.016	6.42%
MBTCP	16752	3598.975	4.655	80.498	1348507	374.692	0.003	1.88%
TCP (only)	798367	3599.845	221.778	116.724	93188406	25886.78	0.207	89.63%
UDP	158	3173.531	0.05	214.62	33910	10.685	0	0.02%
ARP	466	3326.18	0.14	62.009	28896	8.687	0	0.05%

Table 11. Snapshot - heavy external SCADA

	Packets	Time	Avg. Packets/sec	Avg. Packet size (bytes)	Bytes	Avg. bytes/sec	Avg. Mbit/sec	% of total Traffic
Total	1398209	3599.523	388.443	103.238	144348254	40102.054	0.321	
ALL TCP	1396631	3599.523	388.004	103.22	1441660465	40049.883	0.32	0.998871
DNP3	20050	3598.563	5.572	85.002	1704282	473.601	0.0004	1.43%
SMB	58423	3597.637	16.239	128.964	7534471	2094.283	0.017	4.18%
MBTCP	19358	3598.981	5.379	80.492	1558164	432.946	0.003	1.38%
TCP (only)	1299129	3599.486	360.921	102.716	133441212	37072.296	0.297	92.91%
UDP	1005	3250.506	0.309	149.549	150297	46.238	0.000	0.07%
ARP	517	3211.926	0.161	60	31020	9.658	0	0.04%

Table 12. Snapshot - light external SCADA

	Packets	Time	Avg. Packets/sec	Avg. Packet size (bytes)	Bytes	Avg. bytes/sec	Avg. Mbit/sec	% of total Traffic
Total	890446	3599.845	247.357	116.111	103390224	28720.74	0.23	
DNP3	17910	3598.608	4.977	85.004	1522424	423.059	0.003	2.01%
SMB	57171	3593.369	15.91	127.958	7315511	2035.836	0.016	6.42%
MBTCP	16752	3598.975	4.655	80.498	1348507	374.692	0.003	1.88%
TCP (only)	798367	3599.845	221.778	116.724	93188406	25886.78	0.207	89.66%
UDP	95	3173.531	0.03	224.411	21319	6.718	0	0.01%
ARP	232	3326.18	0.07	60	13920	4.185	0	0.03%

Table 13. Aggregate background model - heavy traffic

Type	Average Packet Size (Bytes)	Traffic Load (bps)
ICCP	103.238	321,000
ICS	538.717	2,376,000
Internal	320.9775	196,516,000
External	789.583	13,805,000

Table 14. Aggregate background model - light traffic

Type	Average Packet Size (Bytes)	Traffic Load (bps)
ICCP	116.111	230,000
ICS	116.103	230,000
Internal	466.687	69,902,000
External	621.35	36,415,000

In addition, a generic four port switch supporting network speeds of (up to) 100Mbps was used to provide connectivity from the communication nodes/agent architecture to the routers, guaranteeing complete integration into the long haul infrastructure. Generic Ethernet workstations were used to model the agent architecture.

Physically locating the nodes was a difficult problem. The IEEE common data format file does not give Cartesian coordinates nor does it provide corresponding longitude and latitude to accomplish global positioning. In light of this shortfall a formula developed by Juan Carlos-

Gonzalez was used to efficiently estimate the location of the buses. Although there are too many variables for the calculated measurements to be exact, his work proved that the resulting product was sufficient enough to carry out studies on the power grid. Carlos-Gonzalez' formula $l = R * Area/\rho$ where l =”length,” R=”Branch Resistance,” $Area$ =1.25 in^2 or .00080642 m^2 (cross sectional area of Aluminum) and ρ =”Static Resistivity of Aluminum” (2.50188 x 10^{-8} Ωm). [42] The corresponding OPNET® physical representation for the LAN links is depicted in Figure 23.

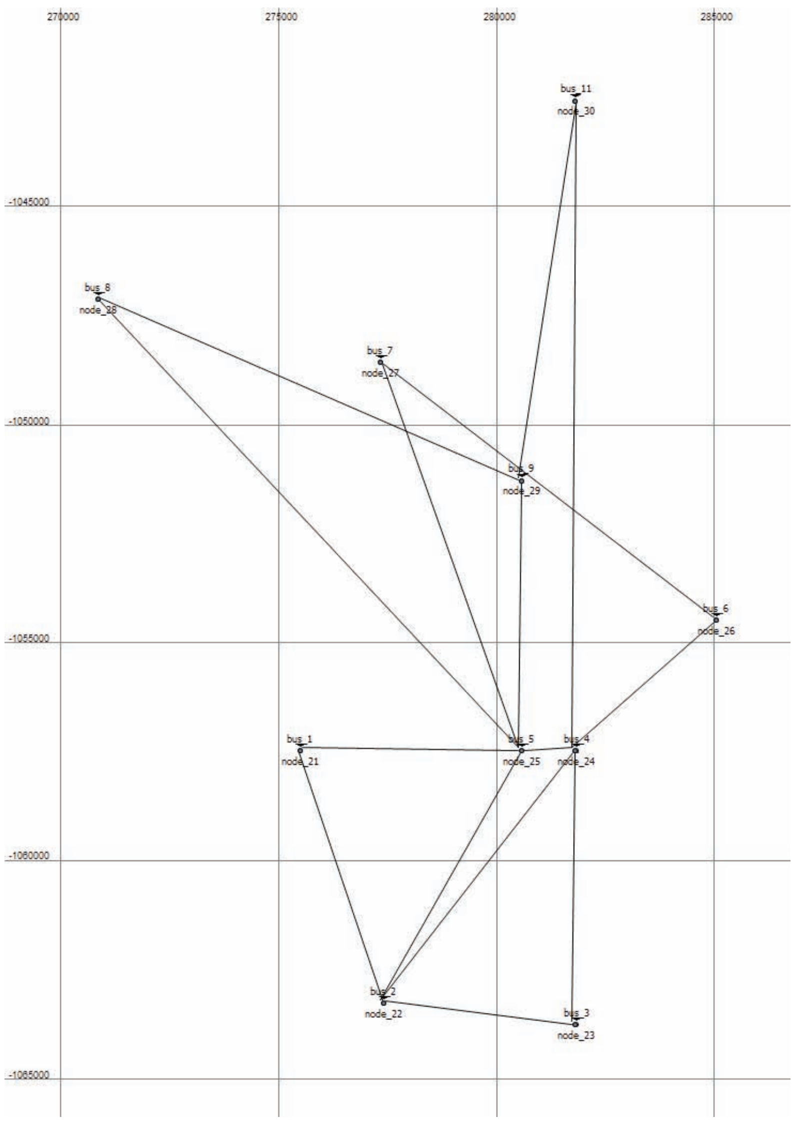


Figure 23. IEEE 14 bus Communications Network

Each individual node (1 - 11) will be modeled to accept input from the external simulation manager. This manager, external to both OPNET® and PowerWorld© has the ability to shuttle data back and forth to either simulation environment via external interfaces. There is an external interface for each type of packet/logic request. See figures on pages 68 and 69 for packet representation. Figure 24 delineates the external module used by OPNET® (shaded in red) and the agent interface (shaded in yellow) that processes the input, makes a decision and then forwards that decision to the simulation manager or another node in the system. Similarly, the area shaded in blue is the seven layer stack that is native to OPNET's workstation model.

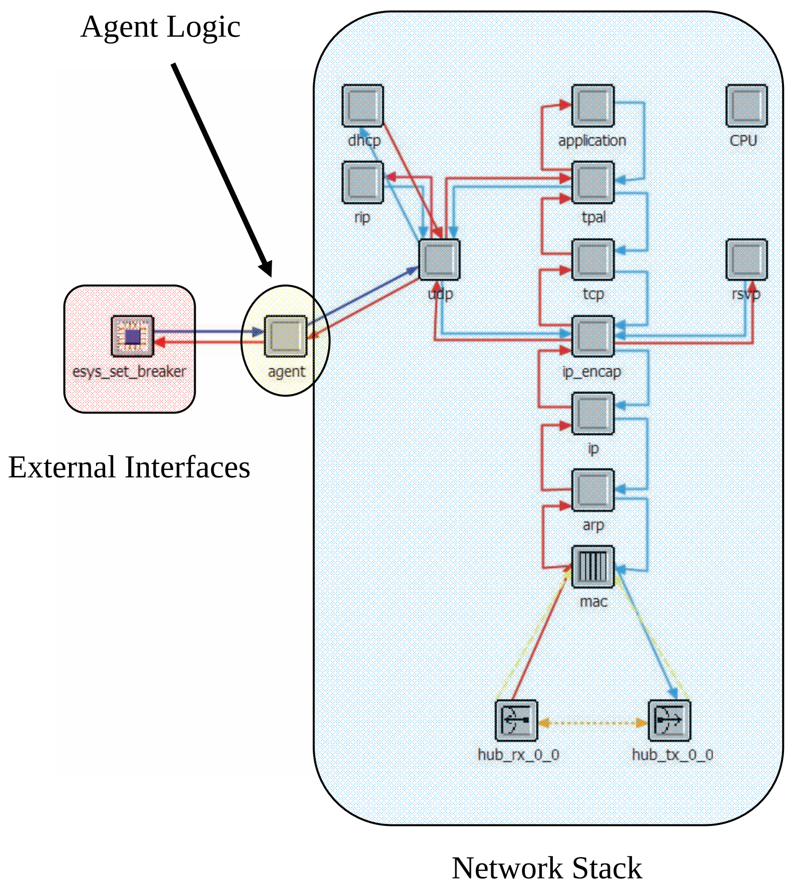
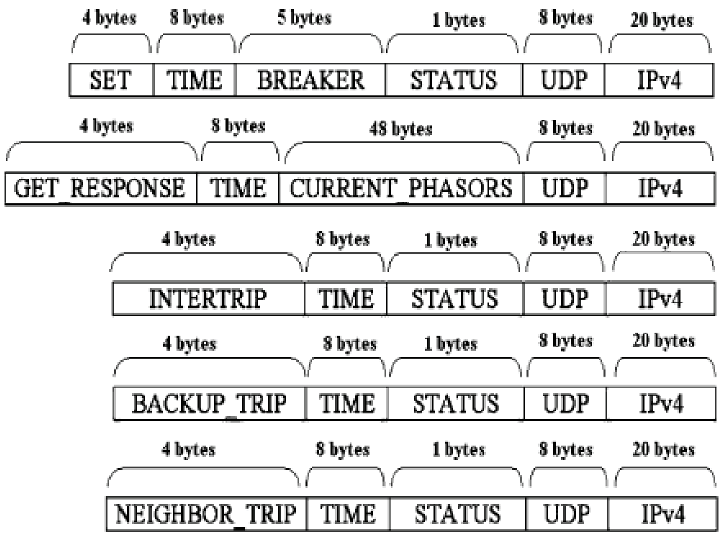


Figure 24. Workstation node model

Previous environments used a custom message structure (Figure 25) for communication amongst the agents.



1. All messages share the first two and last two fields
2. Message one is the command to set the breakers (open/closed)
3. Message two contains the values for the current phasors A, B and C (fault)
4. Message three through four represent the three different kinds of trips present in the system

Figure 25. EPOCHCS Agent Message Structure [41]

Figure 26 on the following page provides a pictorial representation of the following interaction. Representative power data is passed into OPNET® via an array. That array is parsed and the data is inserted into a formatted packet. The formatted packet is then sent to the agent process model. This process model performs the logic and then forwards the packet to the destination nodes for action. See Table 4 for specifics on agent interaction.

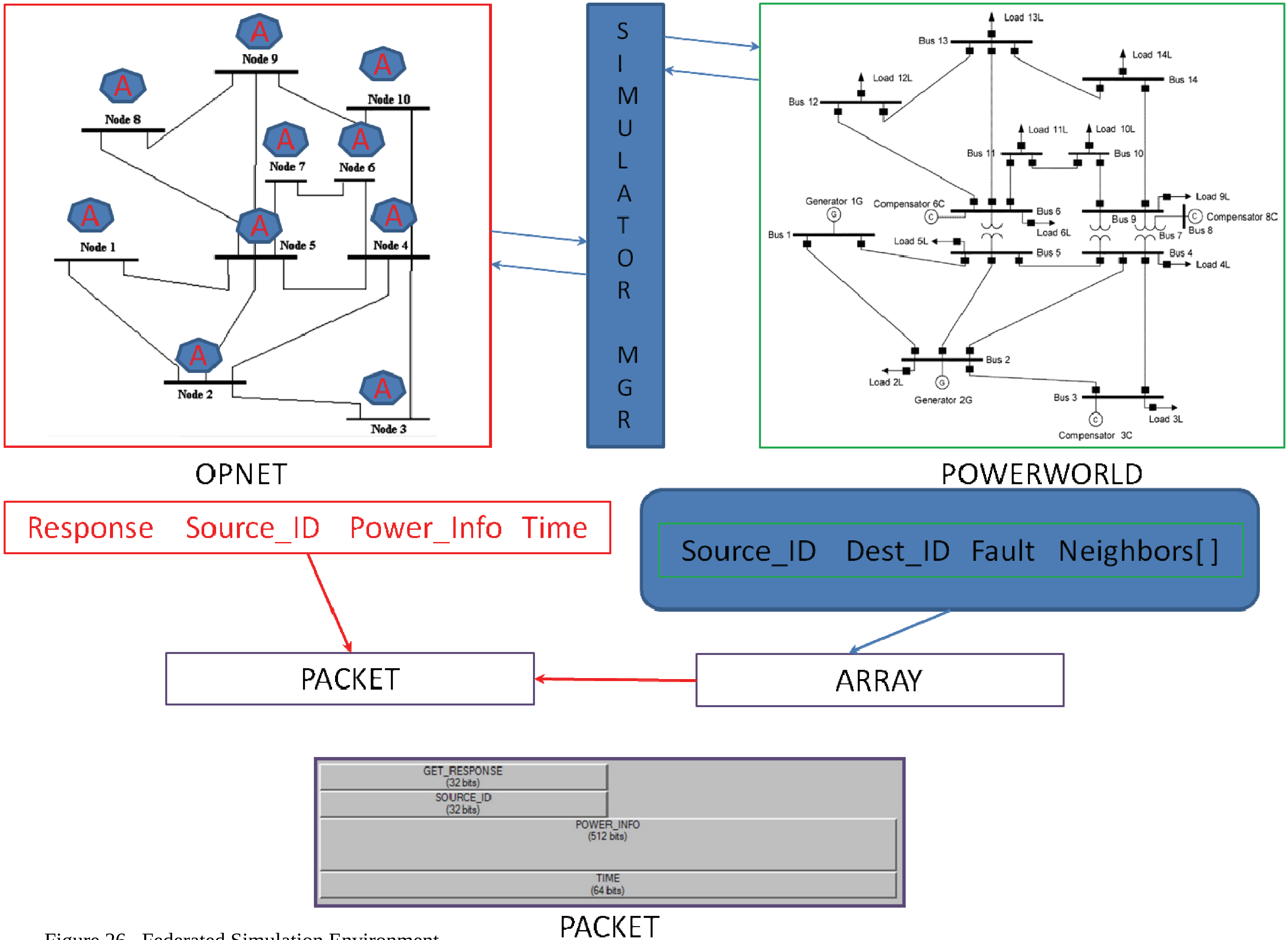


Figure 26. Federated Simulation Environment

Each packet is modeled after the original EPOCHS packet structure. Modifications were made to meet the requirements of the OPNET® and PowerWorld© simulation environment.

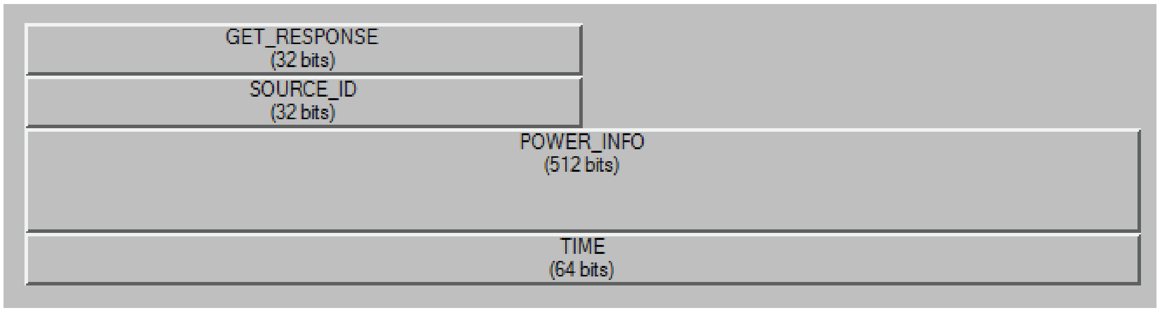


Figure 27. Packet used to get initial feedback from the agent

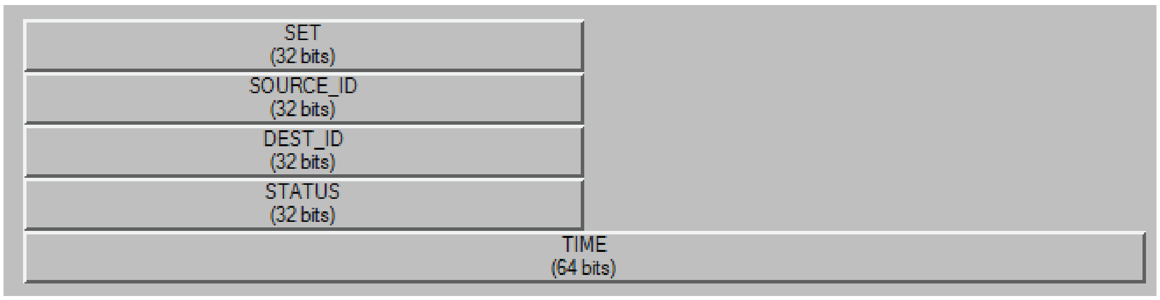


Figure 28. Packet used to execute a source and destination breaker trip

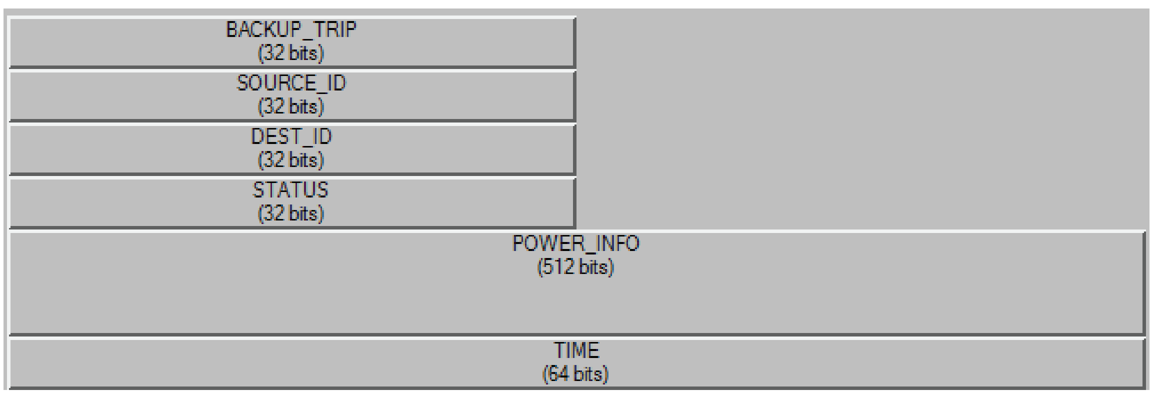


Figure 29. Packet used to send backup trip to internal and external nodes

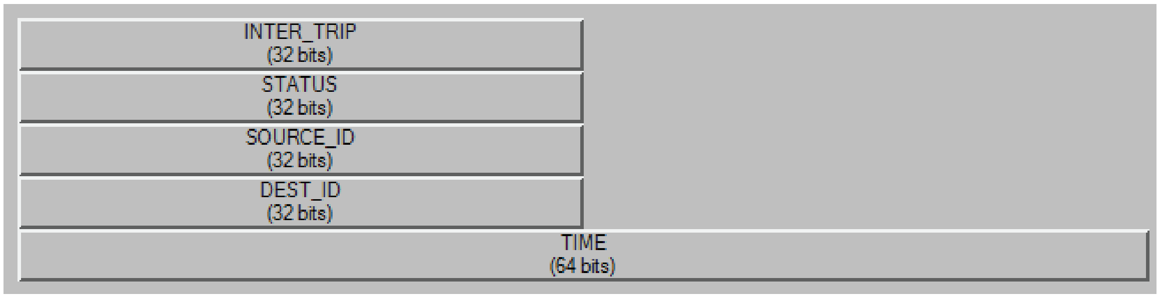


Figure 30. Packet used to execute inter trip

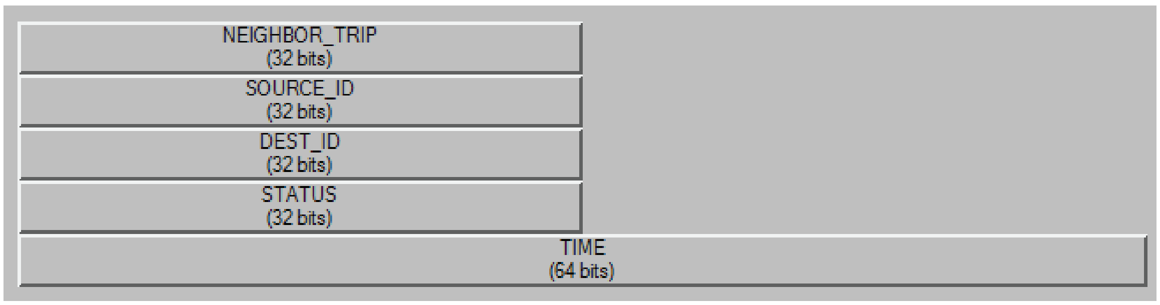


Figure 31. Packet used to execute neighbor trip

Each node's or bus' external interface has a process model that will collect the data and then forward it to the agent process and/or forward it to the external simulation manager. The following figures are Mealy state diagrams (transitions are evaluated on the edges instead of the states) and are representative of the transitions that must evaluate to "true" before some action is taken. Those actions and their transitions are listed in Table 15 for the external interface and Table 16 for the agent.

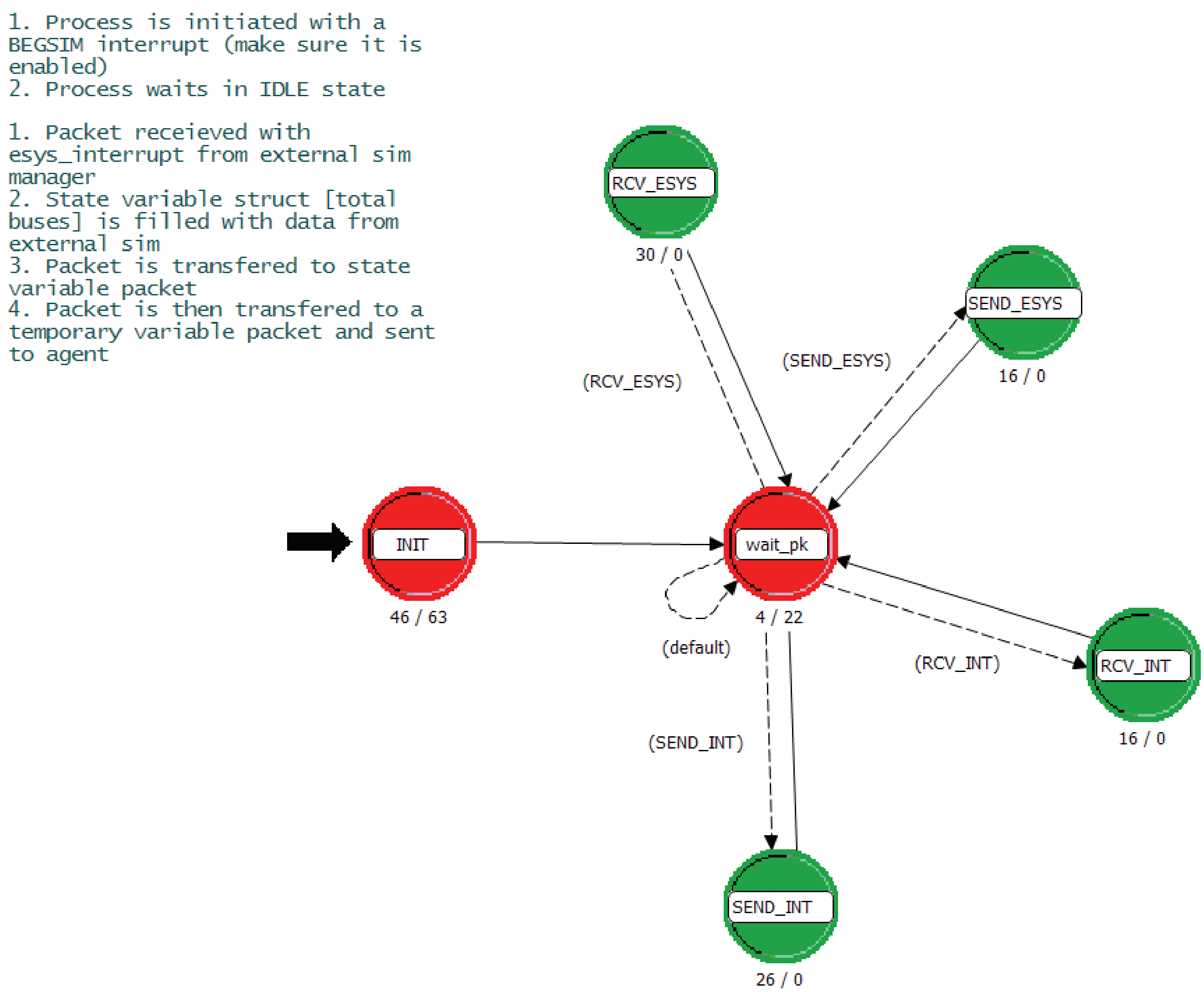


Figure 32. External interface process model

Table 15. External interface Mealy state diagram

INITIAL STATE	TRANSITION STATE	EVENT	ACTION	FINAL STATE
INIT	INIT	BEGSIM INTERRUPT	POWER UP	IDLE
IDLE	RCV_ESYS == TRUE	EXTERNAL INTERRUPT	RECEIVE AND PACKAGE EXTERNAL DATA FROM SIMULATOR	
	SEND_INT == TRUE	STREAM INTERRUPT	SEND DATA TO INTERNAL NETWORK	
	RCV_INT == TRUE	STREAM INTERRUPT	RECEIVE DATA FROM INTERNAL NETWORK AND VERIFY TRIP REQUESTS	
	SEND_ESYS == TRUE	EXTERNAL INTERRUPT	SEND DATA TO EXTERNAL NETWORK FOR ACTION	

Correspondingly, each agent has a process model that gets the packet from the external interface, performs the logic and forwards the packet to the appropriate distant node or gets the packet from a distant node and returns it to the simulation manager.

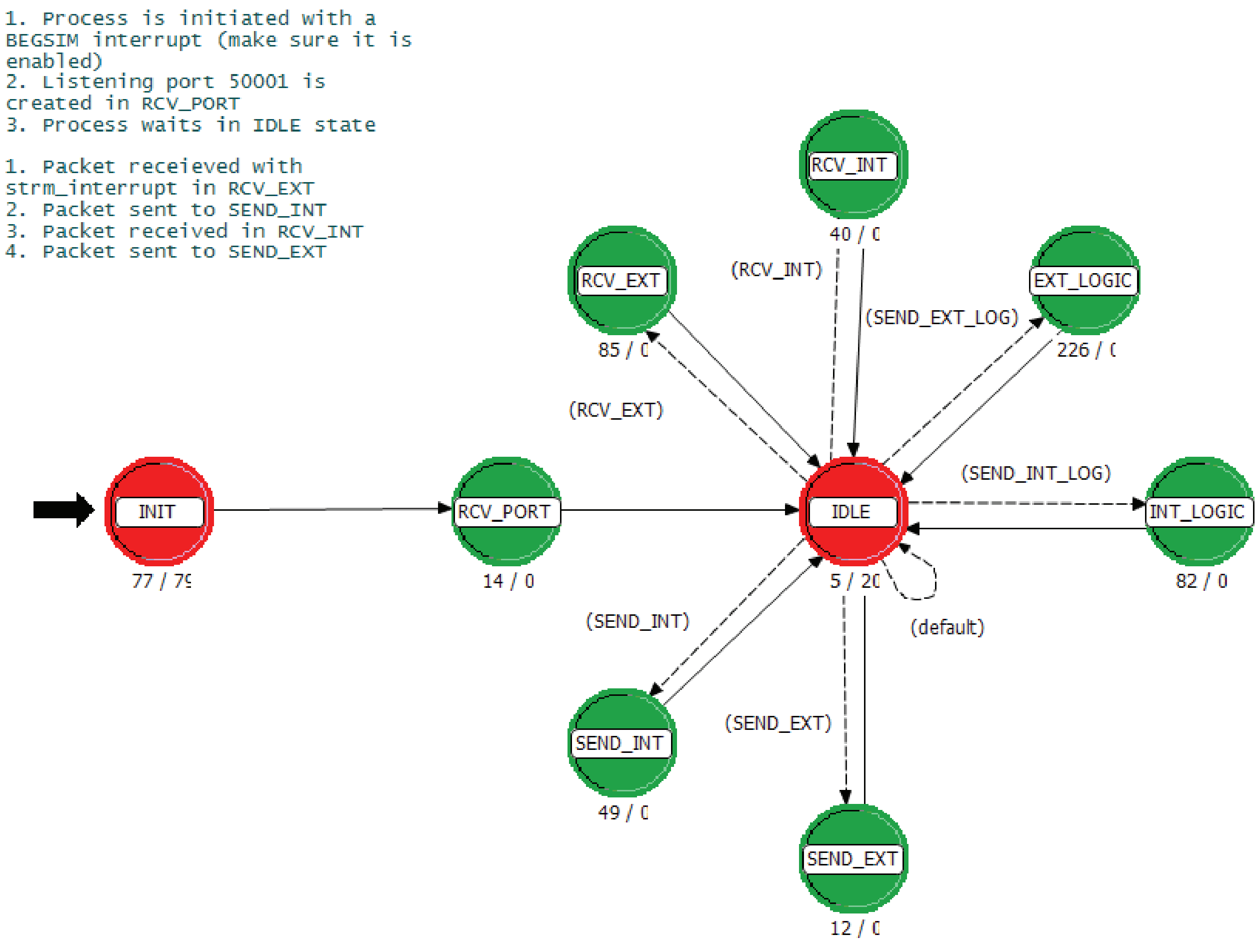


Figure 33. Agent process model

Table 16. Agent final state model

INITIAL STATE	TRANSITION STATE	EVENT	ACTION	FINAL STATE
IDLE	POWER UP	BEGSIM INTERRUPT	INITIALIZE VARIABLES	IDLE
	RCV_PORT	NONE	CREATE RECEIVE PORT	
	RCV_EXT	STREAM INTERRUPT	RECEIVE PACKET FROM SIMULATION MGR PACKAGE DATA FOR PROCESSING	
	EXT_LOGIC	SEND_EXT_LOGIC == TRUE	PERFORM LOGIC TO INDICATE CORRESPONDING TRIP REQUEST AND DESTINATION	
	SEND_INT	SEND_INT == TRUE	SEND TRIP REQUEST TO DESTINATION NODE	
	SEND_EXT	SEND_EXT == TRUE	SEND TRIP REQUEST TO EXTERNAL SIMULATOR	
	RCV_INT	STREAM INTERRUPT	RECEIVE TRIP REQUEST FROM INTERNAL NETWORK	
	INT_LOGIC	SEND_INT_LOGIC == TRUE	PERFORM LOGIC ON TRIP REQUEST RECEIVED FROM INTERNAL SOURCE NODE	

Figure 34 on the next page specifies the corresponding locations or area of responsibility for the four different trips. Accurately predicting and executing the necessary actions needed to bring the power system back to steady state is critical to this process.

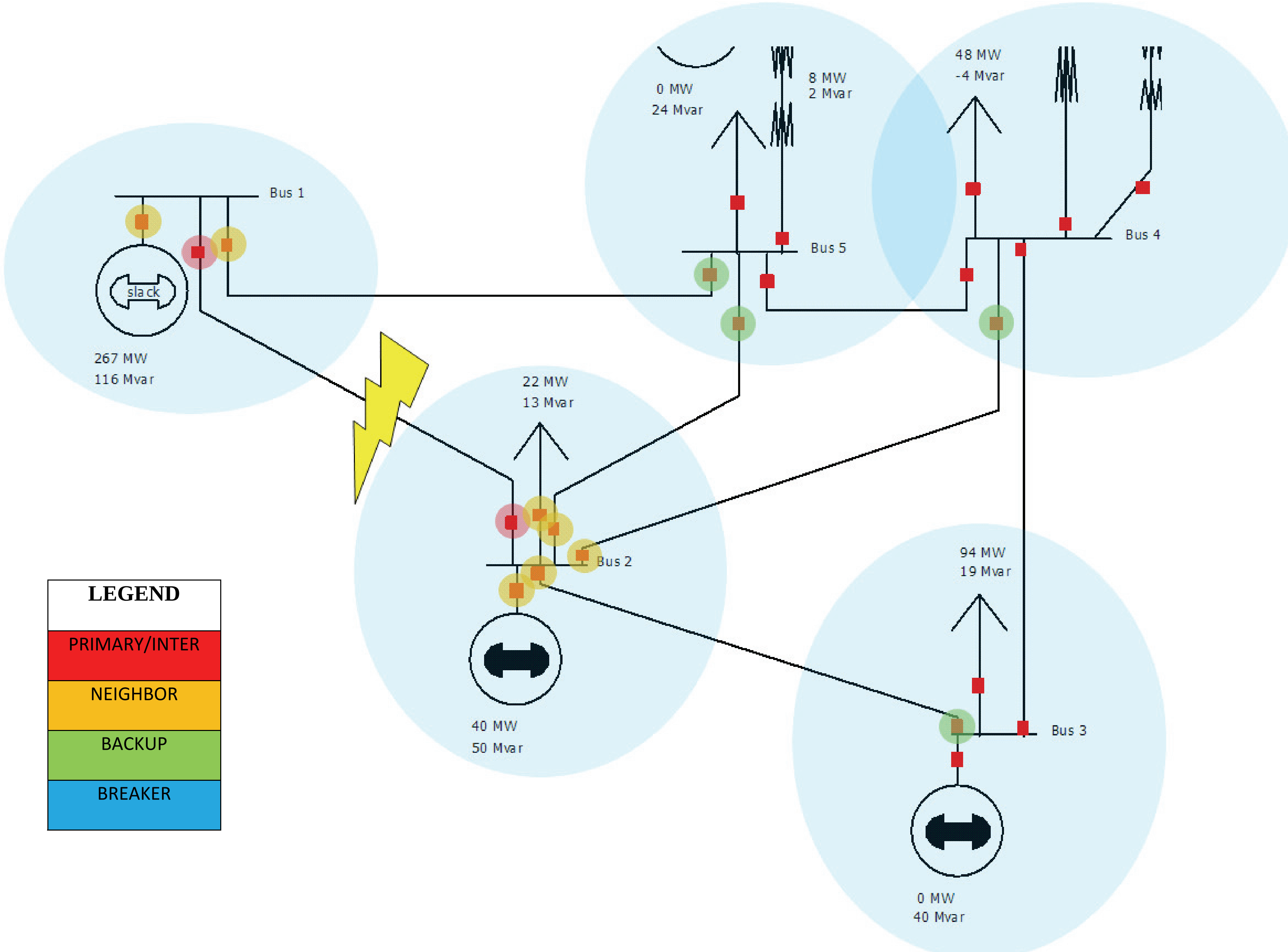


Figure 34. Agent interaction

PowerWorld© has an external library that provides function calls that interact with the power environment. These function calls have the ability to interact and/or solve a static case but does not have the ability to interact with a transient case. At this point in time, the interface was be set up to communicate with PowerWorld©, but dynamic interaction with the external system was nonexistent.

Once the simulation environment was complete a series of experiments were accomplished to test network throughput and agent interaction in a simulated power environment. First, the system was configured to print acknowledgements, receipts and data to verify that the proper communication was taking place. Next, the logic sequences were tested to ensure that the correct requests were being made and if satisfactory they fell within the appropriate bounds. Finally, a measure of end-to-end delay was accomplished to ensure we were theoretically able to resolve the power anomalies within a specified timeframe. OPNET® has native tools that assisted with the calculation of this delay. Upon receipt of the packet in question (at the destination) it's simply a matter of subtracting current time from packet creation time to calculate total end-to-end delay.

Table 17 on the next page was critical to validating the efficacy of the federated simulation environment. It established acceptable time constraints for critical benchmarks in electric utility operations.

Table 17. Time Constraints for Electric Utility Operations [43]

Systems	Situation	Response Time
Substation IEDs; Primary short circuit protection and control	Routine power equipment signal measurement	Every 2-4ms
	Local-area disturbance [6]	< 4ms from event detection to sending notification [14]
		4 - 40 ms automatic response time
SCADA	Emergency event notification	< 6 ms
	Routine transactions	< 540 ms [3]
	Routine HMI status polling from substation field devices	Every 2 secs

Communication delays were measured with and without superimposed LAN traffic. In addition communication delays were measured with protection mechanisms active and the establishment of connected and disconnected communication links. Table 18 lays out all possible simulation tests that could be accomplished during this experiment.

Table 18: Variables under test

Variables under test	Seed	Disrupted Links	Background LAN Traffic	Faults/Trips
Transmission Delay	4 variables with a potential of 24 different base combinations – 4 different traffic loads (100, 125, 150, 175%) – 31 different seeds – 124 different test cases			

A 145 bus IEEE test case was implemented after the initial 14 bus test case had been successfully modeled. In order to emphasize the complexity of the systems, both power and network, the OPNET® and PowerWorld© representations are displayed in Figures 35 and 36. This test case had the ability to represent/model power system transients. However, in our case, it must be noted that PowerWorld© does not currently support this capability.

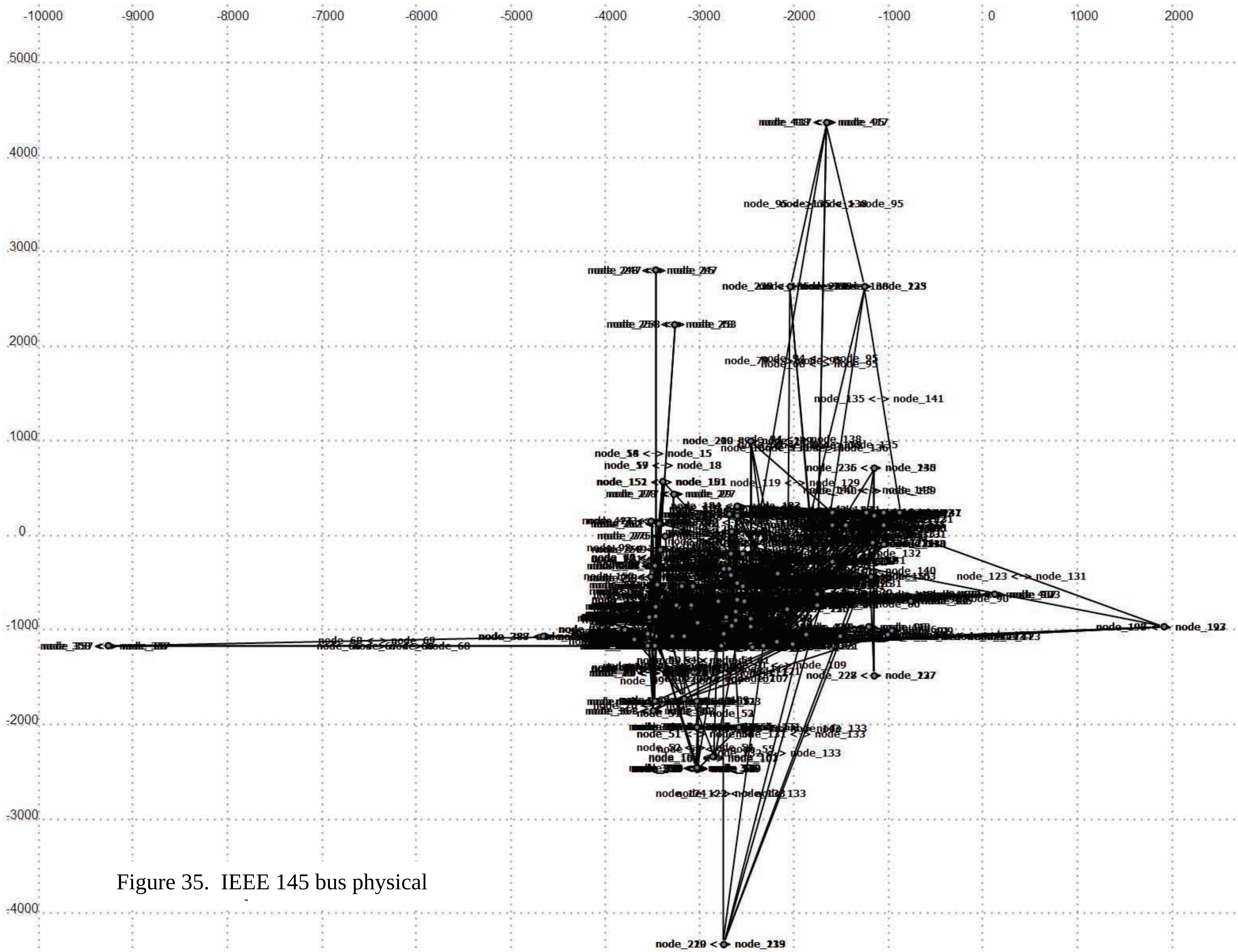


Figure 35. IEEE 145 bus physical

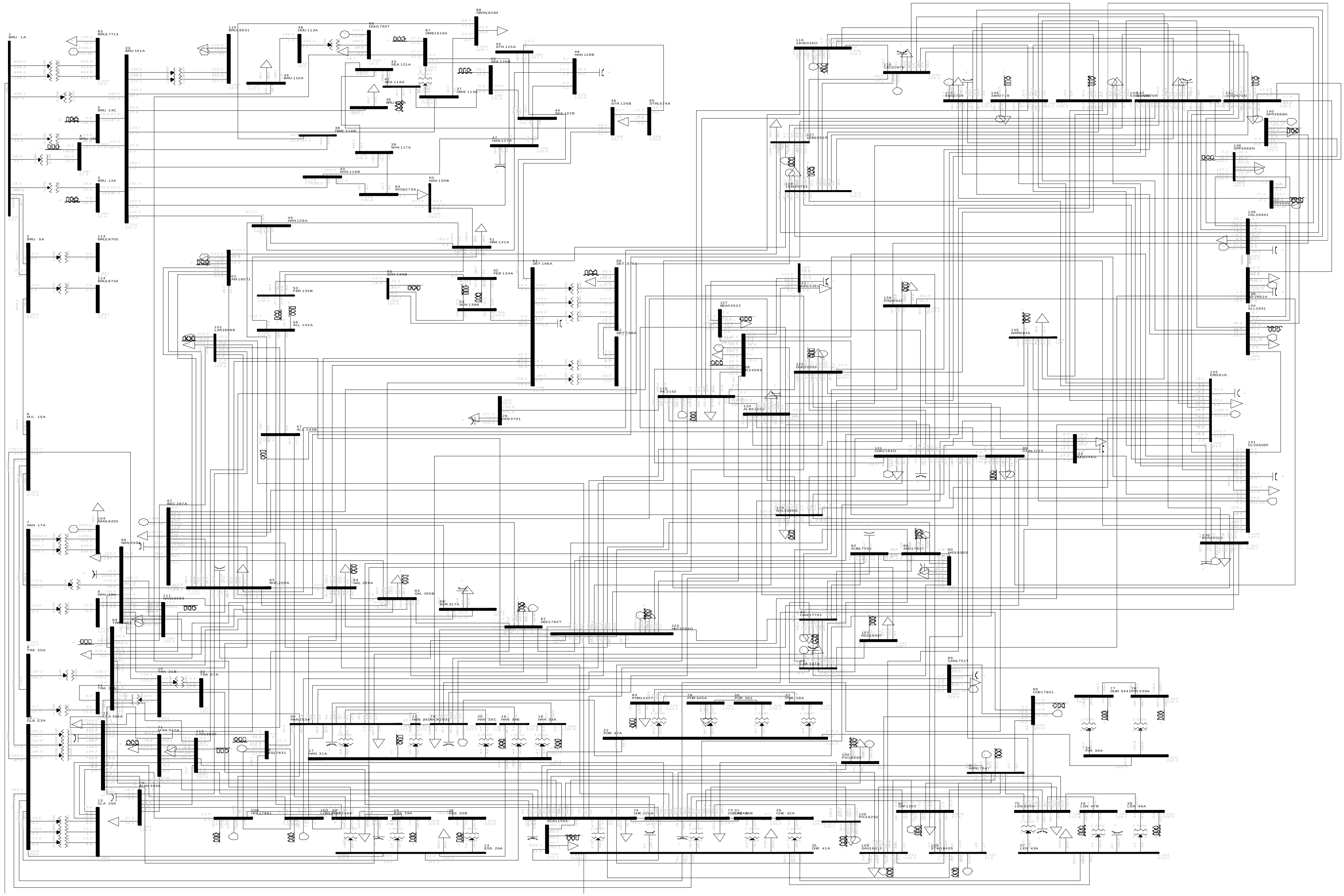


Figure 36. 145 bus IEEE test case

Summary

There are many simulation environments that attempt to model "real" electric environments. Creating a dynamic power system simulation is critical to the development of future power grids. Not only do we have to be able to simulate the effects of power corruption, but we also have to develop a distributed communications network to replicate and study the effects of the communication environment. While this methodology does not attempt to explain previous and on-going work regarding trust nodes and/or agents, it does allow the possibility for the use of these environments regarding future work in this area.

With that said, the work done by the EPOCHS team, while impressive, does not satisfy the need for a visual simulation. Likewise, VCSE is able to create the 3D environment and has the capability to leverage the potential advantage of modeling a dynamic power and communication environment. Taking the best of both worlds and integrating a dynamic simulation with a realistic visual representation allows the industry to prepare for the distributed grid/smart grid revolution. This study attempts to shed light on the capabilities of an agent simulation and the effects of the marriage between traditional grid traffic with a corporate LAN. More specifically, can utility companies trust their LAN to support the rising communication needs of an ever expanding power grid infrastructure?

IV. Analysis and Results

Chapter Overview

The purpose of this chapter is to present the results of the aforementioned methodology. Primarily, the main focus is agent interaction in the presence of what can be considered varying loads of LAN and SCADA traffic. Second to these findings will be an analysis of popular bandwidths and the affect on agent communication. Next will be a comparison of the delay of agent communication and how that's affected by malfunctioning links. Lastly, will be an analysis of the selection of different seeds and how it may or may not affect the results.

Results of Simulation Scenarios

The first simulation was executed using the 14 bus IEEE case. Background traffic consisting of captured LAN and SCADA traffic was placed on all LAN and inter-nodal links. The maximum bandwidth for LAN traffic was 100 Mbps and the selected bandwidth for intermodal links was T1 or 1.544 Mbps. Initial background traffic was light; utilizing the loads that were discussed in Table 14. While running simulations on this particular configuration, link utilization of the LAN links immediately spiked to unacceptable levels. This overutilization can be seen in Table 19. For example, placing 100% of "light" traffic on a T1 link between node_0 and node_1 caused the bidirectional utilization of the link to spike to well over 100%.

Table 19. Detailed link utilization 100% T1 light traffic

	Link Name	Utilization Fwd (%)	Throughput Fwd (Mbps)	Utilization Rtn (%)	Throughput Rtn (Mbps)
1	node_0 <-> node_1	131.11	2.024	123.32	1.904
2	node_1 <-> node_2	138.87	2.144	138.87	2.144
3	node_2 <-> node_3	131.09	2.024	131.09	2.024
4	node_3 <-> node_4	154.41	2.384	162.18	2.504
5	node_4 <-> node_0	138.88	2.144	146.64	2.264
6	node_4 <-> node_6	154.41	2.384	169.96	2.624
7	node_6 <-> node_5	131.09	2.024	115.55	1.784
8	node_5 <-> node_3	169.96	2.624	154.41	2.384
9	node_7 <-> node_8	115.55	1.784	115.55	1.784
10	node_8 <-> node_9	131.09	2.024	131.09	2.024
11	node_9 <-> node_3	154.41	2.384	154.41	2.384
12	node_1 <-> node_4	154.41	2.384	154.41	2.384
13	node_1 <-> node_3	138.87	2.144	131.10	2.024
14	node_8 <-> node_4	154.41	2.384	154.41	2.384
15	node_7 <-> node_4	154.41	2.384	154.41	2.384
16	1 <-> node_20	36.15	36.147	36.15	36.146
17	node_20 <-> node_0	36.15	36.146	36.15	36.147
18	2 <-> node_21	36.15	36.146	36.15	36.146
19	node_21 <-> node_1	36.15	36.146	36.15	36.146
20	3 <-> node_22	36.15	36.146	36.15	36.146
21	node_22 <-> node_2	36.15	36.146	36.15	36.146
22	4 <-> node_23	36.15	36.146	36.15	36.146
23	node_23 <-> node_3	36.15	36.146	36.15	36.146
24	5 <-> node_24	36.15	36.146	36.15	36.146
25	node_24 <-> node_4	36.15	36.146	36.15	36.146
26	7 <-> node_26	36.15	36.146	36.15	36.146
27	node_26 <-> node_6	36.15	36.146	36.15	36.146
28	6 <-> node_25	36.15	36.146	36.15	36.146
29	node_25 <-> node_5	36.15	36.146	36.15	36.146
30	10 <-> node_29	36.15	36.146	36.15	36.146
31	node_29 <-> node_9	36.15	36.146	36.15	36.146
32	9 <-> node_28	36.15	36.146	36.15	36.146
33	node_28 <-> node_8	36.15	36.146	36.15	36.146
34	8 <-> node_27	36.15	36.146	36.15	36.146
35	node_27 <-> node_7	36.15	36.146	36.15	36.146

Correspondingly, Table 20 demonstrates the same overutilization of the links while using just 1/4 of the light traffic load. The table demonstrates that there was no remaining bandwidth left on the links since current bidirectional utilization was well over 100%.

Table 20: Detailed link utilization 25% T1 light traffic

	Link Name	Utilization Fwd (%)	Throughput Fwd (Mbps)	Utilization Rtn (%)	Throughput Rtn (Mbps)
1	node_0 <-> node_1	107.80	1.664	103.89	1.604
2	node_1 <-> node_2	105.84	1.634	105.84	1.634
3	node_2 <-> node_3	111.67	1.724	111.67	1.724
4	node_3 <-> node_4	117.50	1.814	109.72	1.694
5	node_4 <-> node_0	109.74	1.694	113.61	1.754
6	node_4 <-> node_6	119.44	1.844	113.61	1.754
7	node_6 <-> node_5	107.78	1.664	113.61	1.754
8	node_5 <-> node_3	111.67	1.724	117.50	1.814
9	node_7 <-> node_8	103.89	1.604	103.89	1.604
10	node_8 <-> node_9	107.78	1.664	109.72	1.694
11	node_9 <-> node_3	117.50	1.814	115.55	1.784
12	node_1 <-> node_4	109.72	1.694	109.72	1.694
13	node_1 <-> node_3	109.72	1.694	105.84	1.634
14	node_8 <-> node_4	109.72	1.694	111.67	1.724
15	node_7 <-> node_4	113.61	1.754	113.61	1.754
16	1 <-> node_20	9.04	9.038	9.04	9.037
17	node_20 <-> node_0	9.04	9.037	9.04	9.038
18	2 <-> node_21	9.04	9.037	9.04	9.037
19	node_21 <-> node_1	9.04	9.037	9.04	9.037
20	3 <-> node_22	9.04	9.037	9.04	9.037
21	node_22 <-> node_2	9.04	9.037	9.04	9.037
22	4 <-> node_23	9.04	9.037	9.04	9.037
23	node_23 <-> node_3	9.04	9.037	9.04	9.037
24	5 <-> node_24	9.04	9.037	9.04	9.037
25	node_24 <-> node_4	9.04	9.037	9.04	9.037
26	7 <-> node_26	9.04	9.037	9.04	9.037
27	node_26 <-> node_6	9.04	9.037	9.04	9.037
28	6 <-> node_25	9.04	9.037	9.04	9.037
29	node_25 <-> node_5	9.04	9.037	9.04	9.037
30	10 <-> node_29	9.04	9.037	9.04	9.037
31	node_29 <-> node_9	9.04	9.037	9.04	9.037
32	9 <-> node_28	9.04	9.037	9.04	9.037
33	node_28 <-> node_8	9.04	9.037	9.04	9.037
34	8 <-> node_27	9.04	9.037	9.04	9.037
35	node_27 <-> node_7	9.04	9.037	9.04	9.037

Since there was no room for additional traffic (for instance agent traffic) at the diminished rate of just 25% of light LAN traffic (approximately 650 users) it was decided that this scenario was not representative of a realistic benchmark for a corporate LAN.

Subsequently, running experiments on T1 links utilizing the heavy traffic profile was ignored. Immediately, from the results of this initial experiment, one can draw the conclusion that were a utility company to have a similar background traffic profile it may not be realistic or at the very least reasonable for that company to place both their SCADA and user traffic on T1 links.

The next scenario utilized standard LAN bandwidth (100 Mbps) and T3 links with a bandwidth of 44.736 Mbps. The results displayed in Tables 21 and 22 proved that this configuration provided a much more realistic scenario as traffic utilization fell dramatically. Bidirectional background utilization (light traffic) between inter-nodal routers node_0 and node_1 fell from a peak average of 127.215% to 42.04%. That left approximately 26 Mbps of available throughput for use. Likewise, LAN traffic between workstation 1 and the switch named node_20 remained relatively constant at 36% utilization, proving the latter to be a much more acceptable solution. It must be noted that since the length of our T3 links would require the use of numerous repeaters, this was definitely not an exercise in setting up the perfect network. One can easily eliminate the need for repeaters by using fiber links instead. However, you now have the added cost of provisioning a more expensive communications infrastructure.

Table 21. Detailed link utilization 100% T3 light traffic

	Link Name	Utilization Fwd (%)	Throughput Fwd (Mbps)	Utilization Rtn (%)	Throughput Rtn (Mbps)
1	node_0 <-> node_1	41.78	18.691	42.30	18.923
2	node_1 <-> node_2	42.03	18.803	42.03	18.803
3	node_2 <-> node_3	42.30	18.923	42.30	18.923
4	node_3 <-> node_4	43.10	19.283	42.30	18.923
5	node_4 <-> node_0	42.59	19.051	42.03	18.803
6	node_4 <-> node_6	43.37	19.403	42.30	18.923
7	node_6 <-> node_5	41.49	18.563	42.57	19.043
8	node_5 <-> node_3	42.83	19.163	43.91	19.643
9	node_7 <-> node_8	41.49	18.563	41.49	18.563
10	node_8 <-> node_9	42.30	18.923	42.03	18.803
11	node_9 <-> node_3	42.57	19.043	42.83	19.163
12	node_1 <-> node_4	42.57	19.043	42.57	19.043
13	node_1 <-> node_3	42.03	18.803	42.57	19.043
14	node_8 <-> node_4	43.10	19.283	42.83	19.163
15	node_7 <-> node_4	42.83	19.163	42.83	19.163
16	1 <-> node_20	36.17	36.169	36.15	36.146
17	node_20 <-> node_0	36.15	36.146	36.17	36.169
18	2 <-> node_21	36.15	36.146	36.16	36.158
19	node_21 <-> node_1	36.16	36.158	36.15	36.146
20	3 <-> node_22	36.15	36.146	36.15	36.146
21	node_22 <-> node_2	36.15	36.146	36.15	36.146
22	4 <-> node_23	36.15	36.146	36.15	36.146
23	node_23 <-> node_3	36.15	36.146	36.15	36.146
24	5 <-> node_24	36.15	36.146	36.16	36.158
25	node_24 <-> node_4	36.16	36.158	36.15	36.146
26	7 <-> node_26	36.15	36.146	36.15	36.146
27	node_26 <-> node_6	36.15	36.146	36.15	36.146
28	6 <-> node_25	36.15	36.146	36.15	36.146
29	node_25 <-> node_5	36.15	36.146	36.15	36.146
30	10 <-> node_29	36.15	36.146	36.15	36.146
31	node_29 <-> node_9	36.15	36.146	36.15	36.146
32	9 <-> node_28	36.15	36.146	36.15	36.146
33	node_28 <-> node_8	36.15	36.146	36.15	36.146
34	8 <-> node_27	36.15	36.146	36.15	36.146
35	node_27 <-> node_7	36.15	36.146	36.15	36.146

Table 22. Detailed link utilization 100% T3 heavy traffic

	Link Name	Utilization Fwd (%)	Throughput Fwd (Mbps)	Utilization Rtn (%)	Throughput Rtn (Mbps)
1	node_0 <-> node_1	16.60	7.428	16.59	7.423
2	node_1 <-> node_2	16.32	7.303	16.32	7.303
3	node_2 <-> node_3	17.67	7.903	17.67	7.903
4	node_3 <-> node_4	18.47	8.263	18.20	8.143
5	node_4 <-> node_0	17.41	7.788	17.40	7.783
6	node_4 <-> node_6	17.93	8.023	17.67	7.903
7	node_6 <-> node_5	16.59	7.423	16.86	7.543
8	node_5 <-> node_3	17.93	8.023	18.20	8.143
9	node_7 <-> node_8	16.32	7.303	16.32	7.303
10	node_8 <-> node_9	17.13	7.663	17.13	7.663
11	node_9 <-> node_3	17.67	7.903	17.67	7.903
12	node_1 <-> node_4	16.86	7.543	16.86	7.543
13	node_1 <-> node_3	16.86	7.543	16.86	7.543
14	node_8 <-> node_4	17.67	7.903	17.67	7.903
15	node_7 <-> node_4	17.67	7.903	17.67	7.903
16	1 <-> node_20	100.54	100.540	100.53	100.526
17	node_20 <-> node_0	100.53	100.526	100.54	100.540
18	2 <-> node_21	100.53	100.526	100.53	100.533
19	node_21 <-> node_1	100.53	100.533	100.53	100.526
20	3 <-> node_22	100.53	100.526	100.53	100.526
21	node_22 <-> node_2	100.53	100.526	100.53	100.526
22	4 <-> node_23	100.53	100.526	100.53	100.526
23	node_23 <-> node_3	100.53	100.526	100.53	100.526
24	5 <-> node_24	100.53	100.526	100.53	100.533
25	node_24 <-> node_4	100.53	100.533	100.53	100.526
26	7 <-> node_26	100.53	100.526	100.53	100.526
27	node_26 <-> node_6	100.53	100.526	100.53	100.526
28	6 <-> node_25	100.53	100.526	100.53	100.526
29	node_25 <-> node_5	100.53	100.526	100.53	100.526
30	10 <-> node_29	100.53	100.526	100.53	100.526
31	node_29 <-> node_9	100.53	100.526	100.53	100.526
32	9 <-> node_28	100.53	100.526	100.53	100.526
33	node_28 <-> node_8	100.53	100.526	100.53	100.526
34	8 <-> node_27	100.53	100.526	100.53	100.526
35	node_27 <-> node_7	100.53	100.526	100.53	100.526

Table 23. T1 and T3 light traffic utilization in percent

Long Haul Link	T3 light (100%)	T3 light (25%)	T1 light (100%)	T1 light (25%)
	41.78	10.46	131.11	107.8
	42.03	10.51	138.87	105.84
LAN Utilization:	42.3	10.51	131.09	111.67
100 Mbps	43.1	10.78	154.41	117.5
	42.59	10.66	138.88	109.74
	43.37	10.84	154.41	119.44
	41.49	10.37	131.09	107.78
	42.83	10.71	169.96	111.67
	41.49	10.37	115.55	103.89
	42.3	10.57	131.09	107.78
	42.57	10.71	154.41	117.5
	42.57	10.71	154.41	109.72
	42.03	10.51	138.87	109.72
	43.1	10.71	154.41	109.72
	42.83	10.71	154.41	113.61
Avg.	42.42533333	10.60866667	143.5313333	110.892

Table 23 provides a direct comparison of both the T1 and T3 links in the presence of light background traffic. It clearly delineates the unacceptable behavior of the over-utilized T1 links. In addition, the under-utilization of the T3 links while using 25% of the light background traffic is unmistakable at approximately 11%.

Table 24. Comparison of long haul utilization with light traffic

Long Haul Link	T3 light (100%)	T3 light (25%)	T1 light (100%)	T1 light (25%)
	36.17	9.06	36.15	9.04
	36.15	9.04	36.15	9.04
Long Haul	36.15	9.04	36.15	9.04
Utilization:	36.16	9.05	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.16	9.05	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
	36.15	9.04	36.15	9.04
Avg.	36.152	9.042	36.15	9.04

Once again, Table 24 highlights the fact that inter-nodal, long-haul utilization fell well below acceptable “under” utilization standards. Basic design principles state that network traffic that traverses a link that is only 10% utilized costs the user five times as much per bit than if the link were 50% utilized. [44] In lieu of this common practice, the use of 25% light traffic as a viable test case was eliminated; labeled unnecessary and, quite frankly, unrealistic.

Table 25. Comparison of LAN utilization with heavy traffic

Long Haul Link	T3 heavy (100%)	T3 heavy (25%)	T1 heavy (100%)	T1 heavy (25%)
	16.6	4.17	131.43	106.4
LAN Utilization:	16.32	4.22	115.55	105.84
100 Mbps	17.67	4.28	138.86	109.72
	18.47	4.42	162.18	119.44
	17.41	4.37	139.2	112.22
	17.93	4.42	162.18	117.49
	16.59	4.22	131.09	109.72
	17.93	4.55	162.18	113.61
	16.32	4.08	115.55	103.89
	17.13	4.28	138.87	107.78
	17.67	4.35	154.41	109.72
	16.86	4.35	146.64	111.66
	16.86	4.22	138.86	107.78
	17.67	4.48	154.41	117.49
	17.67	4.42	154.41	113.61
Avg.	17.27333333	4.322	143.0546667	111.0913333

In Table 25 the case was made for the use of heavy background traffic (100% and 25% equivalents) on both the T1 and T3 links. Correspondingly, LAN utilization fell dramatically with the use of the T3 links, but once again, under-utilization is quite evident.

Table 26. Comparison of long haul utilization with heavy traffic

Long Haul Link	T3 heavy (100%)	T3 heavy (25%)	T1 heavy (100%)	T1 heavy (25%)
	100.54	25.15	100.54	25.15
	100.53	25.13	100.53	25.13
Long Haul Utilization:	100.53	25.13	100.53	25.13
	100.53	25.14	100.53	25.14
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.14	100.53	25.14
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
	100.53	25.13	100.53	25.13
Avg.	100.5305	25.132	100.5305	25.132

Continuing our analysis, in Table 26, one can clearly see that the long haul links only consume 25% of the available bandwidth, but looking at the previous table the LAN links are saturated. The T3 “heavy” column had 100% utilization between the routers but the LAN traffic remained minimal. Altogether, the combination of over-utilization of the LAN links and the under-utilization of the long-haul links made the selection of heavy background traffic as part of this study impractical.

Before we make the decision about the size of the sample to be measured we had to verify that the packets were, indeed, traversing the network. Rudimentarily, packet contents and status messages were printed to the OPNET® console. But, in order to

substantiate this communication individual statistics were measured and collected at nodes 1, 2 and 5. Figure 37 - 39 displays the number of packets being sent from source node 1 and being received at node 2 and node 5.

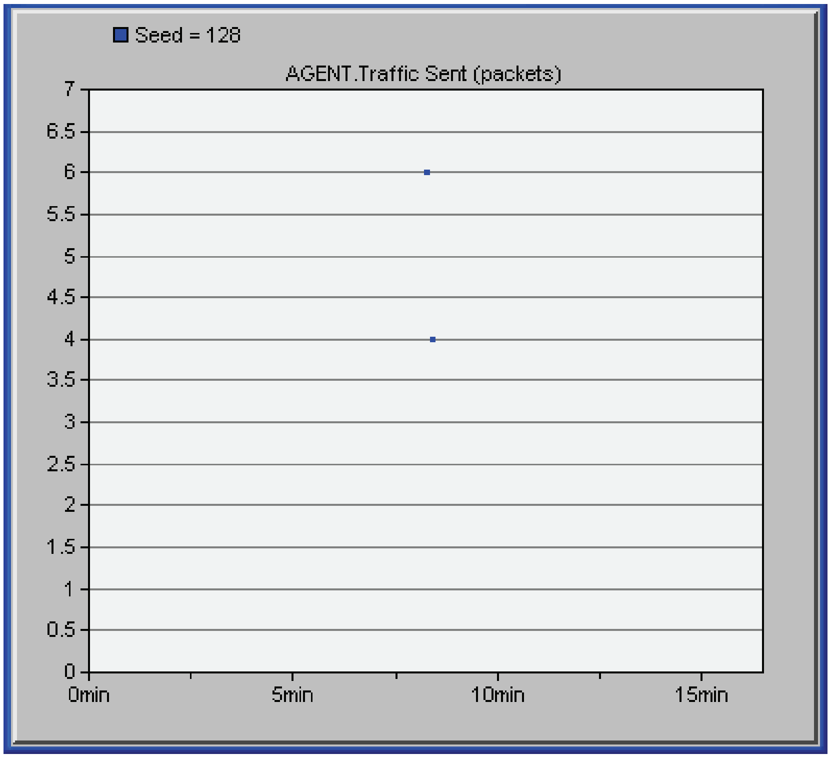


Figure 37. Number of packets sent from bus 1

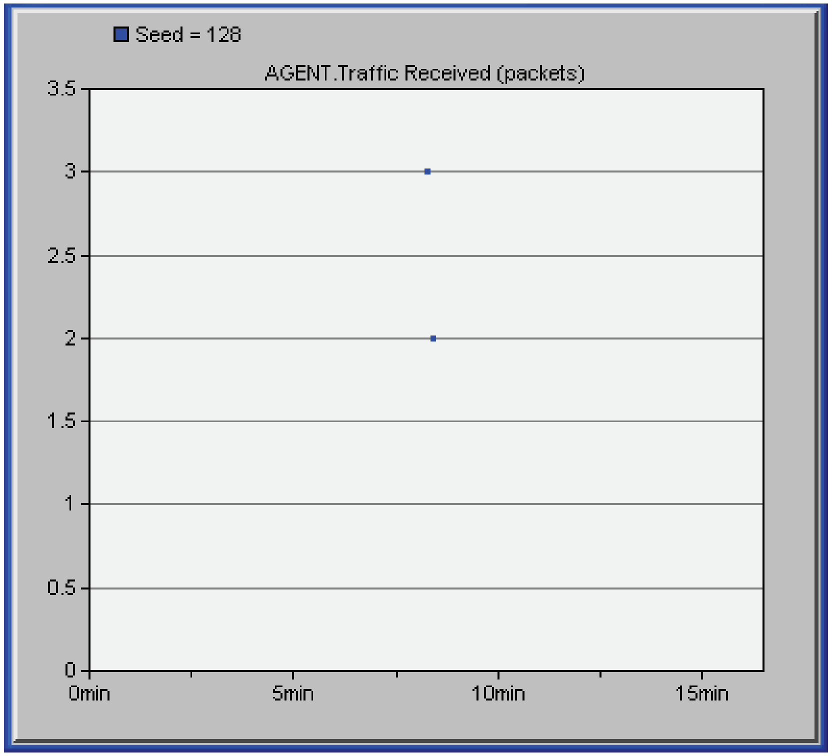


Figure 38. The number of packets received at bus 2

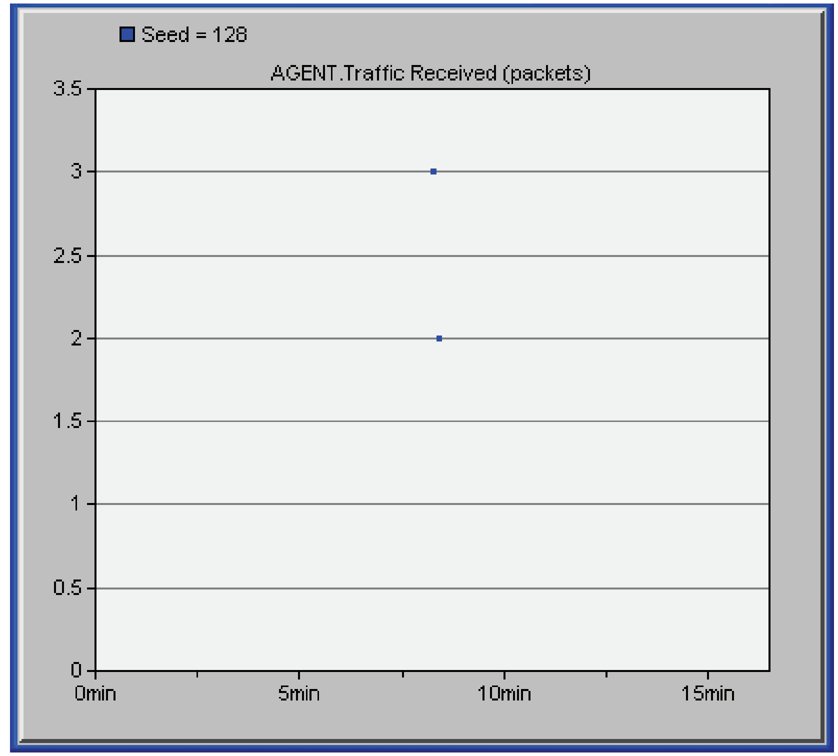


Figure 39. The number of packets received at bus 5

The next decision that needed to be made was the adequacy of the sample size. It is well known that stochastic systems use individual seeds to randomize their results. Since OPNET® inherently models stochastic events a multitude of seeds were chosen to seed their random number generator, producing enough randomized results to provide an adequate confidence level and a relatively narrow confidence interval. Instead of manually calculating sample size, OPNET® has the ability to calculate confidence intervals for the various populations. Initially, simulations were run using 31 random seeds. These seeds were generated non-scientifically or for example – purely by chance. The chosen seeds range from 128 to 512 and increment by 13 giving a total of 30 different seeds. An additional seed of 7255 was chosen to delineate or take into consideration any outliers. The developers of OPNET® recommend several random number seeds to be able to determine standard or typical behavior. [45] The following confidence intervals were calculated by OPNET® and all confidence intervals were calculated at a 95% confidence level.

The following figures display results for agent end-to-end delay. This is the benchmark that will be used to categorically declare our simulation a success or failure. See Table 22 for the specification of these benchmarks. It must be noted that these measurements were taken while observing a breaker trip. An initial response message was sent from the simulation manager to OPNET's external interface. That message was purposely delayed and sent with an offset of 1 second. Since the initial deadline of the response expired, the system will then send a response to trip the breaker at the affected node along with its neighbors. In this case the source node is bus 1 (branch 1 < - > 2) and the neighbors are bus 2 and bus 5. Figures 40 and 41 show the value of end-to-end delay

for all 31 seeds for bus 2 and bus 5. Bus 1 can't display end-to-end delay because no packets were ever sent to that node.

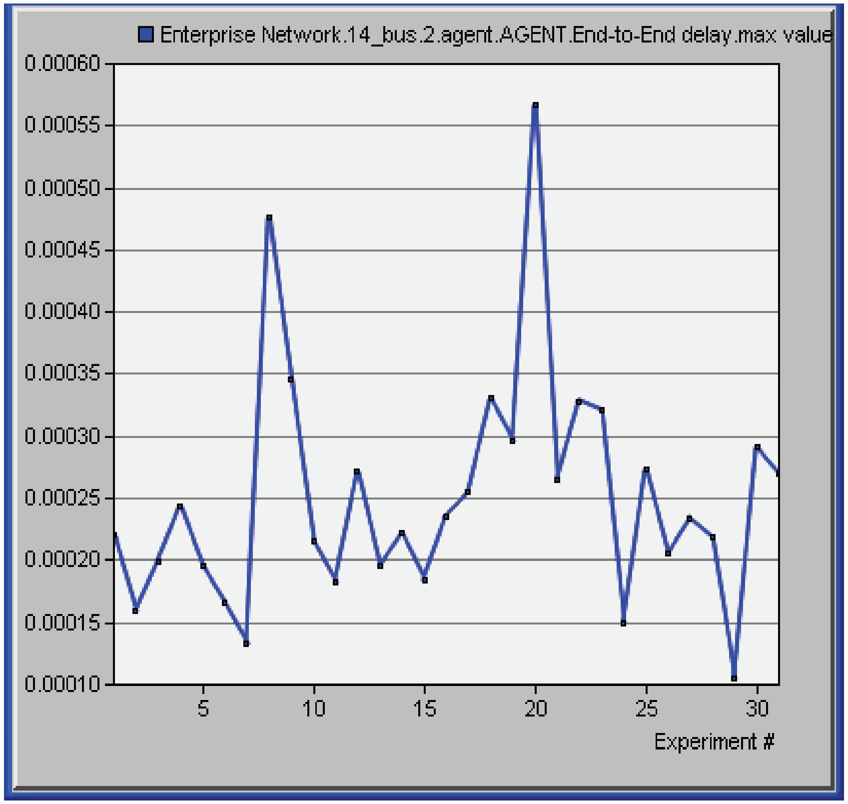


Figure 40. Max Agent end-to-end delay for bus 2 (all 31 seeds)

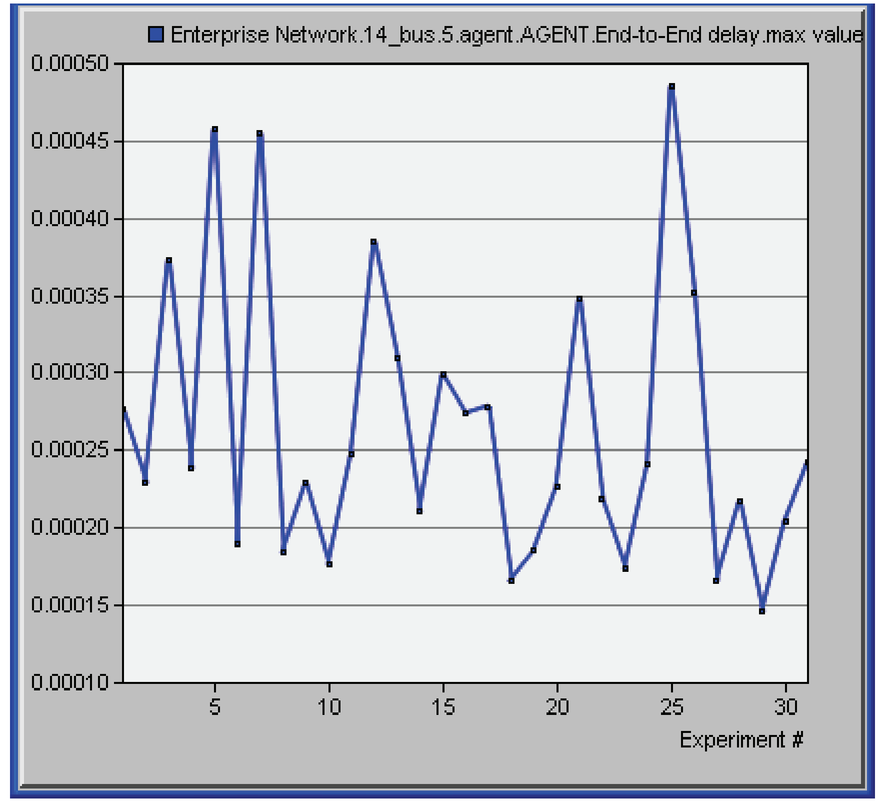


Figure 41. Max Agent end-to-end delay for bus 5 (all 31 seeds)

Figures 42 and 43 display the discrete maximum values for both bus 2 and bus 5.

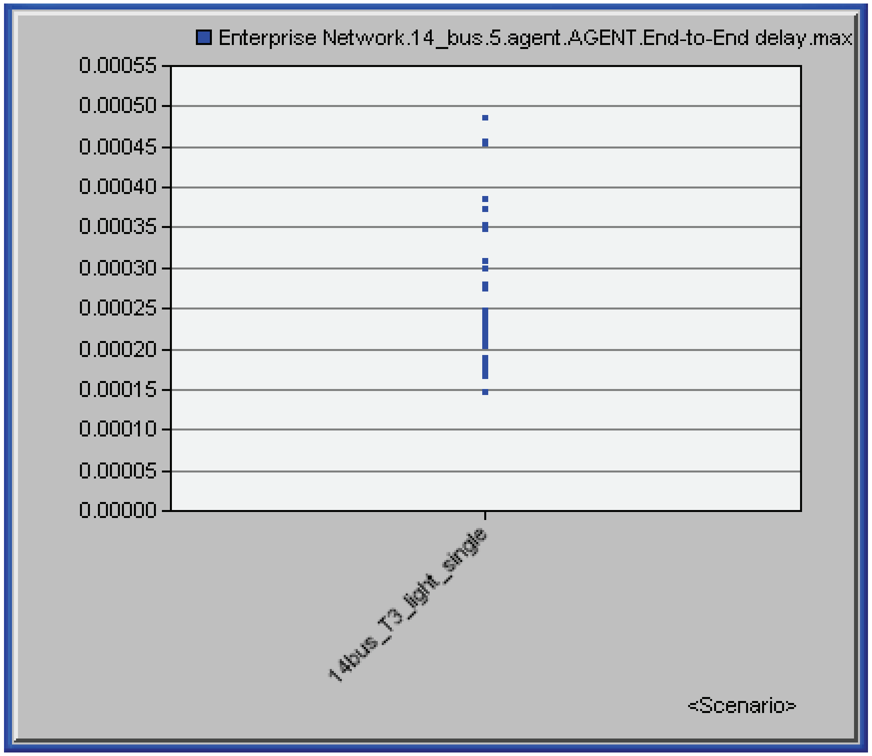


Figure 42. Discrete max Agent end-to-end delay for bus 2 (all 31 seeds)

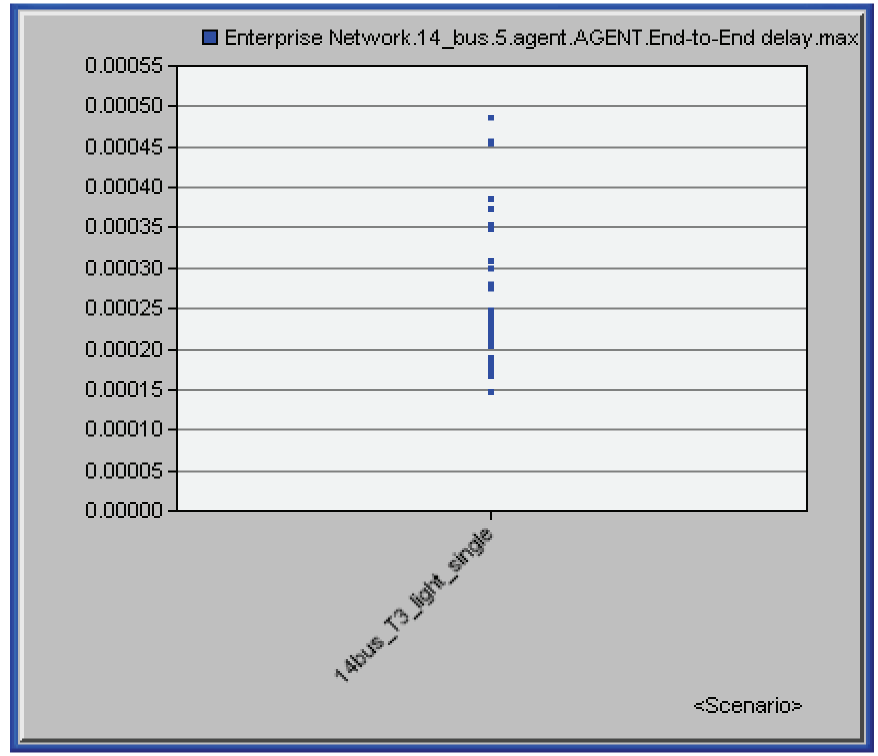


Figure 43. Discrete max Agent end-to-end delay for bus 5 (all 31 seeds)

The following confidence intervals are calculated from the discrete values displayed in the two previous tables.

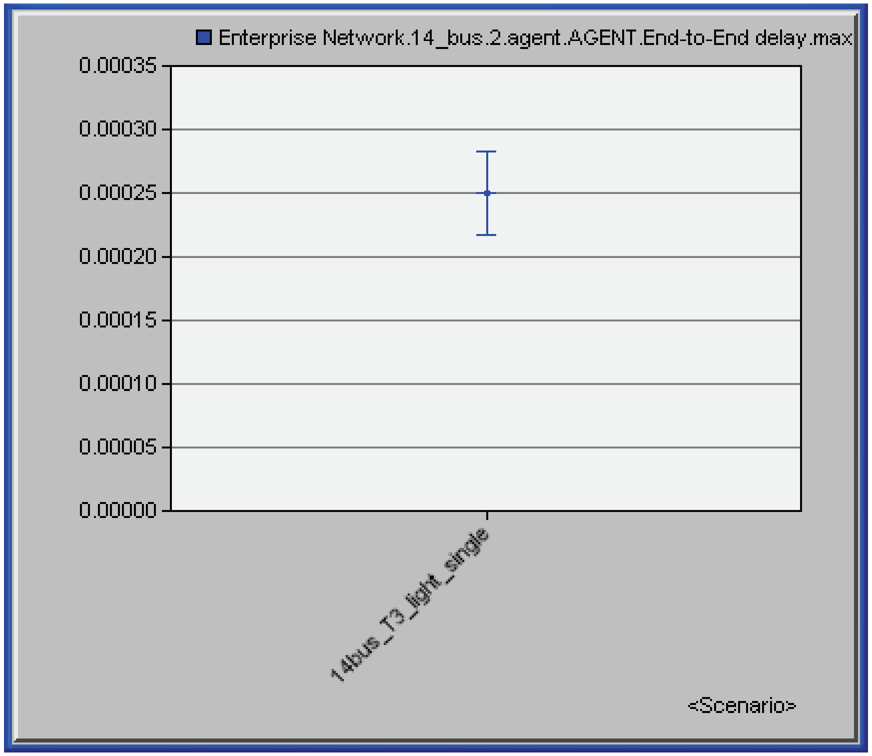


Figure 44. Confidence interval for max Agent end-to-end delay bus 2

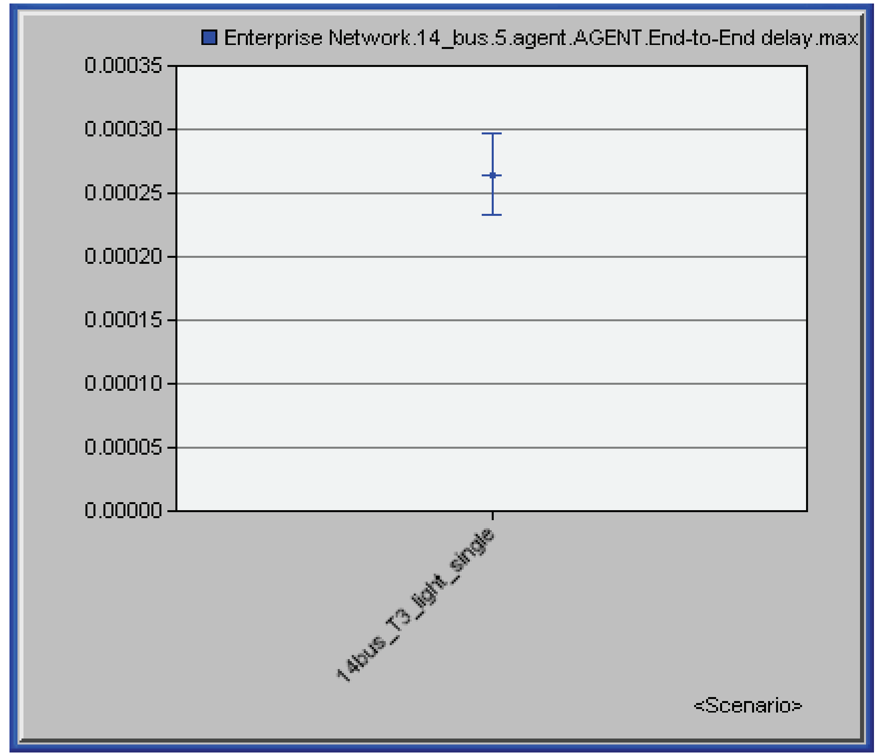


Figure 45. Confidence interval for max Agent end-to-end delay bus 5

The mean of maximum agent end-to-end delay for bus 2 was .00025 seconds and the confidence interval was +/- 3.32561×10^{-5} seconds. Likewise, the mean of maximum agent end-to-end delay for bus 5 was .00026 seconds and the confidence interval was +/- 3.2192×10^{-5} seconds. Again, the confidence level for both these means and intervals was 95%. Statistically, these were very sound numbers. They were relatively close and the intervals were small enough that we could be very confident that these were representative values for the entire population. Looking at our benchmarks in Table 17 we were at least one order of magnitude below our thresholds. Additionally, prior measurements calculate the initial response to the “Get Response” packet to be near instantaneous. In essence, the time that elapses between when the node got the status of the branch and the node’s reply to the response was near zero. This was a valid result because the medium traversed via the coupling of the IED and the power line would be comprised of hardware only. There was no communication medium to slow down the process. The delay that’s measured was only present when the message needed to travel from the source to a corresponding neighbor. That is exactly why, in this experiment, there was no end-to-end delay to be measured on bus 1. The valid conclusion of this first experiment was success.

The second experiment still utilized the same 14 bus case. However, in order to mimic varying degrees of background utilization, background traffic load (T3 light) was varied, using 100, 125, 150 and 175% of the original throughput. This, along with the 31 seeds, led to a total of 124 different simulations. Additionally, a total of ten packets (5 each) and a total of twenty packets (ten each) were sent from source node “bus 1” to

destination nodes “bus 2” and “bus 5.” Table 27 summarizes the end-to-end delay and confidence intervals that were displayed during these runs.

Table 27. 14 bus - 124 runs

124 runs - 31 each	5 Packets		10 Packets	
% of background traffic	Max value end-to-end delay in seconds	Confidence Interval - 95%	Max value end-to-end delay in seconds	Confidence Interval - 95%
100% bus 2	2.50166E-04	3.32561E-05	2.91889E-04	2.93877E-05
100% bus 5	2.64229E-04	3.21920E-05	3.02211E-04	3.01990E-05
125% bus 2	3.19729E-04	3.59127E-05	3.62020E-04	3.52955E-05
125% bus 5	3.24045E-04	3.12615E-05	3.80983E-04	3.84925E-05
150% bus 2	4.35544E-04	2.72579E-05	4.68407E-04	3.45017E-05
150% bus 5	4.71863E-04	6.19943E-05	5.46843E-04	5.63640E-05
175% bus 2	5.54727E-04	5.68313E-05	6.51231E-04	5.68313E-05
175% bus 5	5.99390E-04	6.94843E-05	7.00402E-04	5.41496E-05
Total Traffic	**3.89302E-04**	**2.89182E-05**	**4.82610E-04**	**3.54371E-05**

As expected, looking at the data in Table 27, there was a linear relationship between end-to-end delay of the agent packets and the level of background traffic saturation. However, this delay was still well below the 2 - 4 millisecond threshold and as an aggregate, end-to-end delay was roughly one order of magnitude less than acceptable levels. Likewise, delay was decidedly less when the agent sent fewer packets out on the network; further supporting the argument that, altogether, reduced background and agent traffic led to higher throughput. Again, statistically speaking, these results were quite reliable (95% confidence level) and one could draw the conclusion that this data was representative of the entire population.

The final experiment that was performed on the 14 bus IEEE base case was the loss of a viable link. The link between bus 1 and bus 2 was made inoperable forcing all traffic to be rerouted to branch 1 < - > 5. The idea behind this experiment was to test the

system in the presence of drastically reduced bandwidth; 50% to be exact. Figure 46 displays the precise location of the failed link.

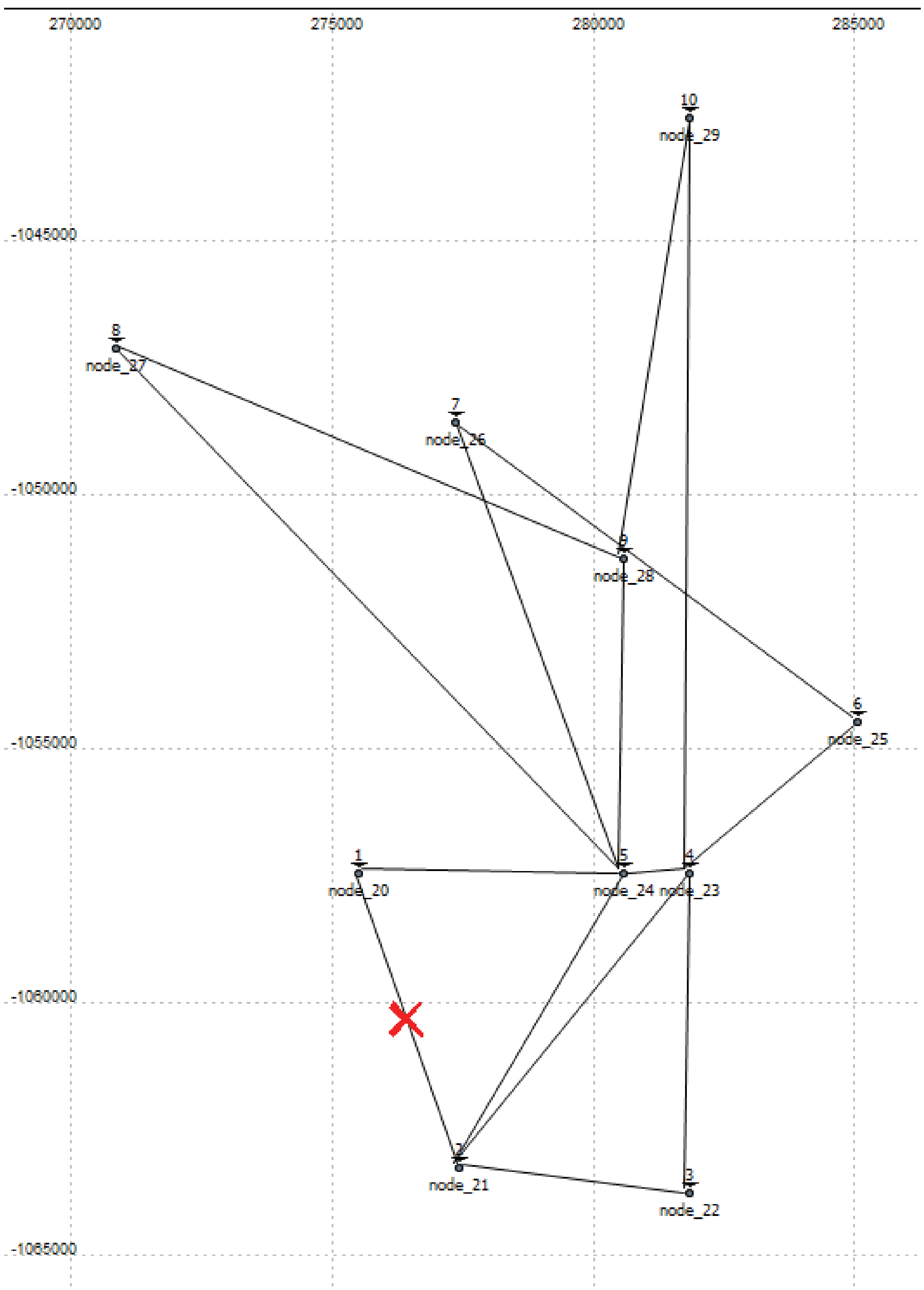


Figure 46. Failed link between bus 1 and 2

Tables 28 through 31 display the system actions taken to affectively shed the load from the disrupted link to the only remaining path. First, Table 28 and 29 exhibit the original bidirectional traffic flows for the branches between bus 1 and 2 (two) and bus 1 and 5 (seven), respectively.

Table 28. Original load for branch 1 < - > 2

	Direction	Bandwidth (Mbps)	Time Period for Peak	Utilization (%)	Throughput (Mbps)	Category	Count
1	node_0 --> node_1	44.736	504.00 - 513.00	41.49	18.563	Traffic Flows	2
2						Applications	2
3						Service Classes	2
4						Traffic Types	2
5							
6	node_1 --> node_0	44.736	169.94 - 171.00	41.49	18.563	Traffic Flows	2
7						Applications	2
8						Service Classes	2
9						Traffic Types	2

Table 29. Original load for branch 1 < - > 5

	Direction	Bandwidth (Mbps)	Time Period for Peak	Utilization (%)	Throughput (Mbps)	Category	Count
1	node_0 --> node_4	44.736	504.00 - 513.00	42.84	19.163	Traffic Flows	7
2						Applications	2
3						Service Classes	2
4						Traffic Types	2
5							
6	node_4 --> node_0	44.736	169.88 - 171.00	42.83	19.163	Traffic Flows	7
7						Applications	2
8						Service Classes	2
9						Traffic Types	2

Tables 30 and 31 reveal the results of the diminished link capacity. The traffic flows for branch 1 < - > 2 diminished from two flows (witnessed in the tables above) to none and the remaining traffic flows on branch 1 < - > 5 was increased from seven to nine. Subsequently, total utilization of the disrupted link fell from approximately .5% while the utilization for the only viable link increased approximately .5%, a relatively even trade-off.

Table 30. Representation of reduced traffic flow and load shedding

	Direction	Bandwidth (Mbps)	Time Period for Peak	Utilization (%)	Throughput (Mbps)	Category	Count
1	node_0 --> node_1	44.736	9.00 - 18.00	40.96	18.323	Traffic Flows	None
2						Applications	2
3						Service Classes	Not Categorized
4						Traffic Types	1
5							
6	node_1 --> node_0	44.736	9.00 - 18.00	40.96	18.323	Traffic Flows	None
7						Applications	2
8						Service Classes	Not Categorized
9						Traffic Types	1

Table 31. Traffic is shed from branch 1 < - > 2 to branch 1 < - > 5

	Direction	Bandwidth (Mbps)	Time Period for Peak	Utilization (%)	Throughput (Mbps)	Category	Count
1	node_0 --> node_4	44.736	504.00 - 513.00	43.37	19.403	Traffic Flows	9
2						Applications	2
3						Service Classes	2
4						Traffic Types	2
5							
6	node_4 --> node_0	44.736	169.97 - 171.00	43.37	19.403	Traffic Flows	9
7						Applications	2
8						Service Classes	2
9						Traffic Types	2

Next, statistics were taken to validate the performance of the agent process in the presence of a less than ideal environment. Table 32 displays the maximum Agent end-to-end delay for both bus 2 and bus 5. The assessment of the results of the 10 packet simulation in Table 27 and that of the simulation in Table 32 reveals an approximate overall average increase of 45.5% in the delay for branch 1 < - > 2 and .63% for branch 1 < - > 5. The increase for the end-to-end delay for all of the agent traffic was 34.52%. The confidence intervals for the data was still tightly bound at a 95% confidence level, leading one to conclude that these results remain statistically significant for this sample of the population.

Table 32. End-to-end delay of nodes with disrupted link at branch 1 < - > 2

	10 Packets	
124 runs - 31 each		
% of background traffic	Max value end-to-end delay in secs	Confidence Interval - 95%
100% bus 2	4.22677E-04	4.22876E-05
100% bus 5	2.97381E-04	1.97485E-05
125% bus 2	4.82841E-04	3.47960E-05
125% bus 5	3.69769E-04	3.66493E-05
150% bus 2	7.36339E-04	8.17095E-05
150% bus 5	5.42452E-04	7.32239E-05
175% bus 2	9.54918E-04	9.63324E-05
175% bus 5	7.55371E-04	9.62825E-05
Total Traffic	**6.49194E-04**	**5.06125E-05**

NOTE: The distance traveled for a packet traveling to bus 2 increased from 6094.99m to 11,163.954m. See Appendix B for IEEE 14 bus PDC results.

Finally, the 145 bus case was implemented using the very same T3 link and traffic setup. Since the science behind the results of the IEEE 14 bus case had already been explored, rudimentary confidence interval calculations and experiments with reduced throughput were not repeated. A 31 sample case with a seed interval of 13 was executed with seeds varying from 128 to 505 and 7255. Additionally, background traffic was varied from 100%, 125%, 150% and 175% of light T3 traffic leading to a total of 124 different scenarios. The results for this experiment are displayed in Table 33.

Table 33. End-to-end delay of nodes with disrupted link at branch 1 < - > 25

124 runs - 31 each	10 Packets	
% of background traffic	**Max value end-to-end delay in secs**	**Confidence Interval - 95%**
100% bus 2	2.49156E-04	2.92175E-05
100% bus 3	2.98871E-04	2.91447E-05
100% bus 4	3.07726E-04	2.88515E-05
100% bus 5	2.95375E-04	2.05169E-05
100% bus 6	3.33282E-04	2.65908E-05
100% bus 25	5.37008E-04	4.36154E-05
100% bus 33	3.56433E-04	2.24274E-05
100% bus 93	3.65967E-04	2.81434E-05
125% bus 2	3.63220E-04	3.60373E-05
125% bus 3	4.01651E-04	4.74785E-05
125% bus 4	3.69188E-04	3.01225E-05
125% bus 5	3.90122E-04	3.88112E-05
125% bus 6	4.37310E-04	5.09470E-05
125% bus 25	6.05542E-04	4.80928E-05
125% bus 33	4.64343E-04	2.91951E-05
125% bus 93	4.43898E-04	4.15097E-05
150% bus 2	4.98510E-04	5.21378E-05
150% bus 3	4.95022E-04	4.60994E-05
150% bus 4	5.12135E-04	5.25940E-05
150% bus 5	5.28221E-04	4.44536E-05
150% bus 6	5.54918E-04	3.44099E-05
150% bus 25	8.68230E-04	7.57888E-05
150% bus 33	5.40811E-04	3.14896E-05
150% bus 93	5.67203E-04	4.89014E-05
175% bus 2	7.02153E-04	8.76746E-05
175% bus 3	6.39760E-04	5.27608E-05
175% bus 4	6.95825E-04	6.94776E-05
175% bus 5	7.10218E-04	5.65988E-05
175% bus 6	7.32467E-04	6.30993E-05
175% bus 25	1.14824E-03	8.82725E-05
175% bus 33	7.38112E-04	5.78665E-05
175% bus 93	7.82017E-04	6.68811E-05
Total traffic	**7.68599E-04**	**6.78289E-05**

In this scenario, the fault in the branch was located between bus 1 and bus 25. Bus 1 has neighbors 2, 3, 4, 5, 6, 25, 33, 93. Like the 14 bus experiment, the inter trip message was delayed causing a breaker trip message to be sent to all its neighbors. End-to-end delay on all the branches got progressively longer, corresponding linearly with the growth of background traffic saturation. For the most part, end-to-end delay remained on the order of one magnitude less than the recommended benchmark, however, the observed delay on branch 1 < - > 25 was significantly close, registering a final value of 1.148 milliseconds .852 less than the 2 millisecond goal. Nevertheless, once again, the response times for this case, like the one before it, remained less than mandated with an overall average of .7686 milliseconds. Correspondingly, the data remained statistically sound with a 95% confidence level and very narrow confidence intervals satisfying the final conclusion that these results were representative of the entire population.

Investigative Questions Answered

OPNET® is able to provide the fidelity to adequately perform and analyze a myriad of networked scenarios. Critical to this investigative work was the correct portrayal and interpretation of end-to-end delay. Without this capability it would have been impossible to ascertain the effectiveness of the EPOCHS like agent. Although one has to incorporate and build the capability to gather these statistics into the model, once collected, analyzing the data becomes a trivial task.

First step is confirming that the data gathered was statistically sound. Common practice is to use the t-statistic when the number of samples is less than thirty and the p-value when the sample size is greater than thirty. There was no need to perform any

rigorous calculations because this practice is inherent to OPNET's statistical analysis module. With just four different seeds and varying the volume of background traffic, attaining 95% confidence in the accuracy of the data was clearly evident. However, with that said, generating and analyzing the results of a thirty member sample was prudent.

Studying network traffic flows is not new science. Upon executing the first case, it was immediately apparent that T1 links were going to be grossly inadequate for the task. LAN link utilization for very light traffic soared over 100%. The fact that this is unsustainable in the real world allowed us to quickly move on to other network configurations. The most realistic options were the utilization of T3 links with 100% of the captured "light" network and SCADA traffic. T3 links had to be used to cover the great distances between the nodes and the use of what was considered bandwidth friendly traffic was still able to adequately portray a relatively robust user base of 500+ employees.

Critical to this work is the accurate measurement and analysis of agent end-to-end delay. Not present in this data is the fact that in prior experiments end-to-end delay appeared abnormally sustained and remained constant throughout various runs. Likewise, that statistic did not vary when a primary link was removed from the system. This inordinate time delay (96 seconds), while evident, was clearly not credible. Link delay on both the 1 to 2 and 1 to 5 links was not significant enough to cause this delay and the distance calculator estimated the current delay between both links to be 16 microseconds. Accordingly, one can safely conclude that the agent was malfunctioning or, in essence, the implementation of the logic was not sound. Corrective measures were

taken to bring the system back to a known good state (reference table 22) and all anomalies regarding the gathering of the critical end-to-end benchmark was corrected.

Likewise, portraying an adequate representation between the power simulator and the network simulator was rudimentary at best. While interaction between the simulators was established, neither transactional data nor any coordinating messages were being passed between the two disparate environments. In fact, during the duration of this study, the capability to perform this type of communication was not an inherent capability of the power simulator. To overcome that shortfall, the simulator manager displayed status messages and updates, provided input to the system and displayed pseudo-messages confirming interaction and communication with both environments.

The addition of the 145 node case proved that a federated simulation environment could adequately be modeled and agent interaction has great potential. Although there are existing implementations of software agents for power simulators, previous to this study none provided the ready functionality of an OPNET® like environment and if they did, they did not scale to this extent. Subsequently, complicated handshaking, scripting and interaction between disparate simulation environments had to be closely coordinated and constantly monitored. Granted, as stated previously, the necessary feedback from the power simulator was absent, but at the very least, the communication pathways were established. This paves the way for some very productive future work.

Summary

The execution of this federated power and communications environment is technically robust and statistically sound. It's both scalable and adaptable. Depending

on the user's need, it can provide a realistic environment to test deployed bandwidth and/or power system interaction. The simulation manager mimics the close coupling of an intelligent electronic device or the more antiquated and specialized remote telemetry units. The manager has the capability to closely coordinate with a power system, eliminating the need for intensive calculations, and then forwarding the status to the agent. The agent provides the logic to the system, making critical decisions to return a corrupt system to steady state. Decision making is near instantaneous and per this implementation, fully redundant. The deployment of the microgrid and the evolution of the smart grid mandate that the power industry plan wisely. Current rates for T1 and T3 lines range from one to three thousand dollars per month. [46] The electric utility industry has the infrastructure to capitalize on the burgeoning Broadband over Power Line technology, providing additional connectivity to support the distribution of bidirectional communication for smart grid installations and the sharing of bandwidth amongst their corporate infrastructure. This research shows that even though this is feasible, extreme care should be taken to ensure a prudent and cost effective decision is made.

V. Conclusions and Recommendations

Chapter Overview

This chapter provides a summary for the research that was performed regarding the implementation of a federated power and communication simulation environment. It discusses future concepts regarding the proposed work and concludes with a discussion for potential future work.

Conclusions of Research

The author concludes that this research successfully federates (combines) both a power and network simulator to provide a tool that will help the power industry successfully plan and execute modern energy initiatives.

Significance of Research

This research attempts to take the best of both worlds, both power and communications, to develop a tool that has the potential to help the utility industry to revolutionize the implementation of their power infrastructure. Often times it's very difficult to accurately forecast the need for additional network bandwidth. With the use of OPNET® as the network simulator engine a myriad of capabilities present themselves to the user. One can plan a full deployment of an entire grid that is spread out over the world or add an addition to their corporate LAN without the loss of fidelity that is often not provided by other network simulators. The graphical user interface (GUI) allows for ease of implementation and execution. The myriad of modules add capabilities that allow engineers to plan their networks down to the minutest detail. Couple that with a power simulator that will eventually have the capability to solve and resolve transient power

anomalies and you have a powerful simulator that can both provide critical network planning alongside another GUI that's easy to use, solving power disruptions and bringing widespread utility networks back to steady state. Though some may claim that this tool already exists, it is the author's belief that existing toolsets are cumbersome, code intensive, antiquated implementations without much documented help or real time support. Additionally, in the event a cutting edge methodology does exist, then more than likely, it's not fully implemented or it's distributed piece-meal on an as needed ad-hoc toolset. With the use of this tool, there is no need to depend on others to plan the expansion of your power network or forecast how your power expansion can affect your existing infrastructure. After the transient mechanism has matured, this tool can easily do both.

Recommendations for Action

The potential of this tool is only limited to the capability of its disparate parts. OPNET® is fully capable and mature. However, PowerWorld© still has to develop key functionality that will assist in solving transient power cases and bringing unstable systems back to acceptable operating limits. The author has recently been made aware that these tools are being released; however the toolsets in question is still in its infancy. It is recommended that this federated system be fully integrated with this new capability and thoroughly tested for any unforeseen anomalies before use.

Recommendations for Future Research

There exists a myriad of potential uses for this toolset, much of which was previously discussed in chapter two and three of this thesis. This federated environment

is very conducive to the study of trust and the implementation thereof. The distributed nature of this environment is perfect for the illumination of difficult trust concepts and once developed, it is fully capable of scaling to any environment. Not only can trust and its associated concepts be thoroughly investigate with this tool, but rudimentary work has already been done on creating subnets that can be easily managed to investigate and discuss associative relationships between nodes, islands and regions. Consequently, the 145 node test case has been segmented using the Power Domain Calculator described in the thesis "Network Security Toolkit Including Heuristic Solutions for Trust System Placement and Network Obfuscation" by Gabriel Greve. [47] Each region can be monitored by a "backup agent", while existing primary agents reside in the regions themselves providing a fully redundant and trusted relationship amongst the peers.

Summary

The need for a sound simulation environment for our power grid infrastructure is significant. Numerous administrations have mandated that our citizenry protect our critical infrastructure. The best way to accomplish that is by ensuring that our power grid has enough network capacity for growth and, at the same time, remains secure. The federated simulation environment can do just that. Provide a way to meet the needs of the industry and the customer while simultaneously meeting the mandates documented in our National Security Strategy.

Appendix A

	Number of domains	Number of Trust Nodes	Domain 1	Domain 2	Domain 3	Domain 4	Domain 5	Domain 6	Domain 7	Domain 8	Domain 9	Domain 10	Domain 11	Avg Domain Size	Real Avg	Standard Deviation	Variance
600/200/1/Round 5	7	102	19	17	23	22	26	19	19					20.714	20.714	3.093772547	9.571428571
600/200/2/Round 17	7	89	25	29	16	22	25	26	25					24.000	20.714	4.082482905	16.66666667
600/200/3/Round 2	7	102	19	17	23	22	26	19	19					20.714	20.714	3.093772547	9.571428571
600/200/4/Round 12	7	102	26	19	17	23	22	19	19					20.714	20.714	3.093772547	9.571428571
600/200/5/Round 12	11	98	16	17	13	8	10	15	5	17	17	15	12	13.182	13.182	4.045199175	16.36363636
200/200/1/Round 8	6	92	33	41	28	26	28	20						29.333	24.167	7.089898918	50.26666667
200/200/2/Round 6	7	98	27	21	20	16	21	25	18					21.143	20.714	3.804758925	14.47619048
200/200/3/Round 16	8	97	26	10	12	11	12	24	36	16				18.375	18.125	9.349369727	87.41071429
200/200/4/Round 7	7	102	19	17	23	22	26	19	19					20.714	20.714	3.093772547	9.571428571
200/200/5/Round 19	7	102	26	19	17	23	22	19	19					20.714	20.714	3.093772547	9.571428571
600/50/1/Round 7	7	45	13	21	30	16	16	24	25					20.714	20.714	6.047431568	36.57142857
600/50/2/Round 10	6	48	21	27	21	30	28	19						24.333	24.167	4.546060566	20.66666667
600/50/3/Round 4	7	39	20	18	10	26	34	24	13					20.714	20.714	8.138678961	66.23809524
600/50/4/Round 16	7	37	32	21	13	16	18	13	32					20.714	20.714	8.199883855	67.23809524
600/50/5/Round 2	6	46	22	27	39	21	14	22						24.167	24.167	8.376554582	70.16666667
200/50/1/Round 3	6	46	22	27	39	21	14	22						24.167	24.167	8.376554582	70.16666667
200/50/2/Round 1	7	49	13	37	25	20	12	13	25					20.714	20.714	9.105205209	82.9047619
200/50/3/Round 12	7	49	10	34	11	27	26	26	11					20.714	20.714	9.793097666	95.9047619
200/50/4/Round 20	5	46	27	31	31	41	15							29.000	29.000	9.38083152	88
200/50/5/Round 19	6	43	13	24	25	25	28	30						24.167	24.167	5.913261931	34.96666667

Trust agent communication in microseconds:
600/200 microseconds
.6 milliseconds
.006 seconds
maximum trust node count of 600 and 200 respectively

Power Domain Calculator’s Subnet

Appendix B

Source	Dest	Distance (m)	Conversion	Distance (mi)	Delay (µs)		Bus	Coordinates of comm node	
Branch								X	Y
1	2	6094.99	0.000621371	3.787251202	16.908		1	275496	-1057500
1	5	5068.964	0.000621371	3.149708203	16.908		2	277409	-1063287
2	3	4408.488	0.000621371	2.739307443	14.705		3	281823	-1063787
2	4	5451.74	0.000621371	3.387554182	18.185		4	281823	-1057500
2	5	5342.911	0.000621371	3.319930977	17.822		5	280571	-1057500
3	4	6286.716	0.000621371	3.906384215	20.97		6	285046	-1054516
4	5	1252.465	0.000621371	0.77824567	4.178		7	277340	-1048590
4	7	0	0.000621371	0	1		8	270845	-1047143
4	9	0	0.000621371	0	1		9	280563	-1051294
5	6	0	0.000621371	0	1		10	281815	-1042591
6	11	8910.794	0.000621371	5.536910689	29.723				
6	12	11531.119	0.000621371	7.165105158	38.464				
6	13	6206.033	0.000621371	3.856250123	20.701				
7	8	0	0.000621371	0	1			T1 max = 6200 feet	
7	9	0	0.000621371	0	1			OC3 mm = 1.2 mi	
9	10	2984.337	0.000621371	1.854381039	9.955			OC3 sm = 9.3 mi	
9	14	11925.153	0.000621371	7.409946534	39.778				
10	11	7697.733	0.000621371	4.78314953	25.677				
12	13	20726.181	0.000621371	12.87865179	69.135				
13	14	16036.24	0.000621371	9.964457564	53.491				
Total Avg		**5996.1932**		**3.725861716**	**20.08**				

14bus coordinate information

Appendix C - 1

Buses	Branches	Distance	Delay	Buses	Branches	Distance	Delay
1	2	2.815	0.009	12	25	47.847	0.16
1	3	844.358	2.816	12	25	47.847	0.16
1	4	844.358	2.816	12	72	28.145	0.094
1	5	834.976	2.785	12	72	28.145	0.094
1	6	182.006	0.607	12	72	28.145	0.094
1	33	9.382	0.031	13	72	18.764	0.063
1	93	18.764	0.063	13	72	28.145	0.094
1	93	18.764	0.063	13	72	18.764	0.063
2	6	182.006	0.607	14	15	3893.43	12.987
2	113	0	1	14	16	938.176	3.129
2	114	16.887	0.056	14	17	318.042	1.061
3	33	18.764	0.063	14	17	330.238	1.102
4	33	18.764	0.063	14	58	18.764	0.063
5	33	18.764	0.063	15	58	18.764	0.063
6	7	121.025	0.404	16	58	18.764	0.063
6	9	15.011	0.05	17	18	29843.37	99.547
6	10	15.011	0.05	17	19	0	1
6	12	18.764	0.063	17	20	0	1
6	12	18.764	0.063	17	21	891.267	2.973
7	8	1050.757	3.505	17	22	213.904	0.714
7	66	14.073	0.047	17	59	9.382	0.031
7	104	33.774	0.113	18	59	18.764	0.063
7	104	38.465	0.128	19	59	0	1
8	66	18.764	0.063	20	59	0	1
8	66	18.764	0.063	21	59	18.764	0.063
9	11	2035.842	6.791	22	23	0	1
9	69	37.527	0.125	22	24	162.304	0.541
10	32	2533.075	8.449	22	30	0	1
10	69	37.527	0.125	22	78	0	1
11	69	18.764	0.063	22	83	0	1
12	13	2092.132	6.979	23	83	37.527	0.125
12	13	2223.477	7.417	23	83	28.145	0.094
12	13	2223.477	7.417	24	76	18.764	0.063
12	14	90.065	0.3	24	77	215.78	0.72
12	14	90.065	0.3	25	26	562.906	1.878

145 bus PDC Data

Appendix C - 2

Buses	Branches	Distance	Delay	Buses	Branches	Distance	Delay
25	27	215.78	0.72	42	44	0.938	0.003
25	27	215.78	0.72	43	46	579.793	1.934
25	31	769.304	2.566	44	45	579.793	1.934
25	73	28.145	0.094	45	61	417.488	1.393
25	74	37.527	0.125	45	85	0	1
26	73	28.145	0.094	46	61	417.488	1.393
27	28	10817.167	36.082	46	85	0	1
27	29	1529.227	5.101	47	48	938.176	3.129
27	75	15.011	0.05	47	50	0.938	0.003
28	75	18.764	0.063	47	87	7796.241	26.005
29	75	18.764	0.063	48	49	0.938	0.003
30	78	0	1	48	87	9362.995	31.232
31	74	28.145	0.094	49	51	842.482	2.81
32	69	18.764	0.063	50	51	842.482	2.81
33	34	5.629	0.019	51	52	272.071	0.908
33	35	5.629	0.019	51	53	272.071	0.908
33	37	934.423	3.117	51	56	712.075	2.375
33	38	933.485	3.114	51	57	712.075	2.375
33	39	797.449	2.66	52	53	628.578	2.097
33	40	796.511	2.657	52	54	440.943	1.471
33	49	525.378	1.752	53	55	440.943	1.471
33	50	525.378	1.752	54	55	5188.112	17.306
33	110	22.516	0.075	54	61	132.283	0.441
33	110	21.578	0.072	55	61	132.283	0.441
34	36	23.454	0.078	56	57	844.358	2.816
36	99	75.054	0.25	56	58	178.253	0.595
37	87	87.25	0.291	57	58	178.253	0.595
37	88	290.835	0.97	58	59	62613.856	208.857
38	88	290.835	0.97	58	72	2833.291	9.451
39	43	564.782	1.884	58	87	8096.457	27.007
39	84	677.363	2.259	58	98	1229.01	4.1
40	44	565.72	1.887	58	100	11192.438	37.334
40	84	683.93	2.281	58	103	78956.879	263.372
41	42	46.909	0.156	59	60	16915.31	56.423
41	43	0.938	0.003	59	72	80805.085	269.537

145 bus PDC Data

Appendix C - 3

Buses	Branches	Distance	Delay	Buses	Branches	Distance	Delay
59	79	928.794	3.098	63	102	1003.848	3.348
59	80	26981.937	90.002	63	102	975.703	3.255
59	89	32094.995	107.057	63	116	36560.712	121.953
59	92	656.723	2.191	63	117	281.453	0.939
59	94	66056.961	220.342	63	118	1172.72	3.912
59	98	9944.664	33.172	63	124	11867.924	39.587
59	100	1716.862	5.727	64	65	121.963	0.407
59	103	3452.487	11.516	64	66	365.889	1.22
59	107	3490.014	11.641	64	67	2185.95	7.292
60	135	171779.996	572.996	64	69	703.632	2.347
60	79	3518.159	11.735	64	97	40679.304	135.692
60	80	6145.052	20.498	64	124	9766.41	32.577
60	90	1885.733	6.29	65	66	365.889	1.22
60	92	24767.842	82.617	65	67	2185.95	7.292
60	94	112.581	0.376	65	69	703.632	2.347
60	95	8021.403	26.757	65	97	40266.507	134.315
60	138	34140.219	113.88	65	124	9681.975	32.296
61	62	3396.197	11.328	66	67	759.922	2.535
61	62	4428.19	14.771	66	68	232010.885	773.905
61	63	761.799	2.541	66	69	262.689	0.876
61	63	761.799	2.541	66	97	10498.188	35.018
61	64	227.039	0.757	66	111	0	1
61	65	227.039	0.757	66	111	53.476	0.178
61	86	123.839	0.413	66	111	0	1
61	86	103.199	0.344	66	111	53.476	0.178
61	86	103.199	0.344	66	124	2655.038	8.856
62	86	337.743	1.127	67	68	323013.942	1077.459
62	86	121.963	0.407	67	69	572.287	1.909
63	64	1379.118	4.6	67	97	591.051	1.972
63	65	1379.118	4.6	67	119	20761.831	69.254
63	66	525.378	1.752	67	120	318.98	1.064
63	67	3011.544	10.045	67	121	769.304	2.566
63	69	1003.848	3.348	67	122	440.943	1.471
63	102	994.466	3.317	67	124	28.145	0.094
63	102	994.466	3.317	67	125	581.669	1.94

145 bus PDC Data

Appendix C - 4

Buses	Branches	Distance	Delay	Buses	Branches	Distance	Delay
67	132	29965.336	99.954	73	101	412.797	1.377
68	69	64921.768	216.556	73	105	65.672	0.219
69	70	797.449	2.66	73	105	65.672	0.219
69	71	703.632	2.347	73	105	56.291	0.188
69	72	121.963	0.407	73	108	1707.48	5.696
69	73	919.412	3.067	73	109	4916.041	16.398
69	74	1266.537	4.225	73	112	403.416	1.346
69	97	6323.305	21.092	73	121	2514.311	8.387
69	101	1632.426	5.445	74	75	2017.078	6.728
69	112	1641.808	5.476	74	81	3124.126	10.421
69	124	2504.929	8.356	74	82	919.412	3.067
70	71	45886.18	153.06	74	91	3874.666	12.924
70	72	581.669	1.94	74	96	40810.649	136.13
70	73	3977.866	13.269	74	101	3227.325	10.765
70	74	300.216	1.001	74	106	281.453	0.939
70	101	11708.434	39.055	74	106	46.909	0.156
70	112	11792.87	39.337	74	108	1754.389	5.852
71	72	562.906	1.878	74	109	9419.285	31.419
71	73	3837.139	12.799	74	112	3236.707	10.796
71	74	168.872	0.563	74	121	3264.852	10.89
71	101	14935.759	49.82	75	82	7289.626	24.316
71	112	15038.959	50.165	75	91	21155.865	70.568
72	73	140.726	0.469	75	96	42368.021	141.325
72	74	262.689	0.876	75	108	394.034	1.314
72	98	1294.683	4.319	75	109	9813.319	32.734
72	100	12543.411	41.84	75	121	1669.953	5.57
72	101	18.764	0.063	76	77	18.764	0.063
72	103	95919.098	319.952	76	89	103.199	0.344
72	112	18.764	0.063	79	80	4127.974	13.769
73	74	65.672	0.219	79	90	4747.17	15.835
73	75	1379.118	4.6	79	92	159.49	0.532
73	81	1144.575	3.818	79	94	11961.742	39.9
73	82	337.743	1.127	79	95	28614.363	95.447
73	91	2542.457	8.481	79	107	7374.062	24.597
73	96	2298.531	7.667	80	90	43700.231	145.768

145 bus PDC Data

Appendix C - 5

Buses	Branches	Distance	Delay	Buses	Branches	Distance	Delay
80	92	11183.056	37.303	116	118	93.818	0.313
80	94	43156.089	143.953	116	143	20517.906	68.44
82	91	22037.75	73.51	117	118	75.054	0.25
82	108	6961.265	23.22	117	143	7824.387	26.099
82	109	666.105	2.222	118	131	83732.194	279.301
82	121	17750.287	59.209	118	132	65362.711	218.027
83	89	5460.183	18.213	118	143	103.199	0.344
89	103	100666.268	335.787	119	120	93.818	0.313
90	92	12946.827	43.186	119	121	1031.993	3.442
90	94	6464.032	21.562	119	122	56412.513	188.172
91	96	11483.272	38.304	119	124	24561.443	81.928
91	108	10113.536	33.735	119	125	769.304	2.566
91	109	25321.366	84.463	119	126	143.541	0.479
91	121	27432.262	91.504	119	127	10995.421	36.677
92	94	27047.609	90.221	119	128	506.615	1.69
92	107	1651.189	5.508	119	129	318.98	1.064
94	95	5009.859	16.711	119	130	206.399	0.688
94	138	10554.478	35.206	119	131	412.797	1.377
95	138	6867.447	22.907	119	132	38812.335	129.464
96	108	77071.145	257.082	119	144	79848.146	266.345
97	124	35585.01	118.699	120	121	84.436	0.282
98	100	591.051	1.972	120	122	5722.873	19.089
98	103	5103.677	17.024	120	123	4371.899	14.583
100	103	2336.058	7.792	120	124	2429.875	8.105
101	112	1294.683	4.319	120	125	18.764	0.063
102	117	28.145	0.094	120	127	187.635	0.626
102	118	2504.929	8.356	120	128	272.071	0.908
108	109	7739.951	25.818	120	129	2148.423	7.166
108	121	84.436	0.282	120	130	15705.064	52.386
109	121	17647.088	58.864	120	131	6445.268	21.499
115	116	75.054	0.25	120	132	2392.348	7.98
115	117	863.122	2.879	121	122	1013.23	3.38
115	118	412.797	1.377	121	123	16061.57	53.576
115	143	9541.248	31.826	121	124	562.906	1.878
116	117	179.192	0.598	121	125	0	1

145 bus PDC Data

Appendix C - 6

Buses	Branches	Distance	Delay	Buses	Branches	Distance	Delay
121	127	1913.879	6.384	130	144	70663.404	235.708
121	128	2608.129	8.7	131	132	300.216	1.001
121	129	42640.092	142.232	131	133	101041.538	337.038
121	131	20480.379	68.315	131	143	5516.474	18.401
121	132	12271.34	40.933	131	144	206.399	0.688
122	123	54789.469	182.758	132	133	8593.691	28.665
122	124	84.436	0.282	132	143	459.706	1.533
122	125	647.341	2.159	132	144	10394.988	34.674
122	131	22825.818	76.139	133	143	33774.33	112.659
122	132	1754.389	5.852	134	131	37921.067	126.491
122	133	9194.123	30.668	134	136	6548.467	21.843
122	143	2927.109	9.764	134	139	3311.761	11.047
123	124	20921.321	69.786	134	141	2157.804	7.198
123	125	7702.424	25.693	134	142	2467.402	8.23
123	131	16727.675	55.798	134	144	1360.355	4.538
123	132	12712.283	42.404	134	145	318.98	1.064
124	125	159.49	0.532	135	95	32348.303	107.902
124	128	108171.674	360.822	135	136	290.835	0.97
124	131	9963.427	33.234	135	138	788.068	2.629
124	132	881.885	2.942	135	141	12102.468	40.369
124	133	3208.561	10.703	136	115	1125.811	3.755
124	143	731.777	2.441	136	116	112581.101	375.53
125	127	7420.971	24.754	136	117	278544.407	929.124
125	128	5816.69	19.402	136	118	53935.729	179.91
125	129	39562.875	131.968	136	138	14832.56	49.476
125	130	185195.911	617.747	136	139	553.524	1.846
125	131	11736.58	39.149	136	140	225443.654	751.999
125	132	5028.623	16.774	136	141	243.926	0.814
127	128	243.926	0.814	136	142	4381.281	14.614
127	129	3677.649	12.267	136	143	165306.583	551.403
128	129	93.818	0.313	136	145	459.706	1.533
128	130	103199.342	344.236	137	139	1716.862	5.727
128	131	146261.613	487.876	137	140	209119.395	697.547
130	131	253.307	0.845	137	145	7993.258	26.663
130	132	61065.865	203.694	139	140	506.615	1.69

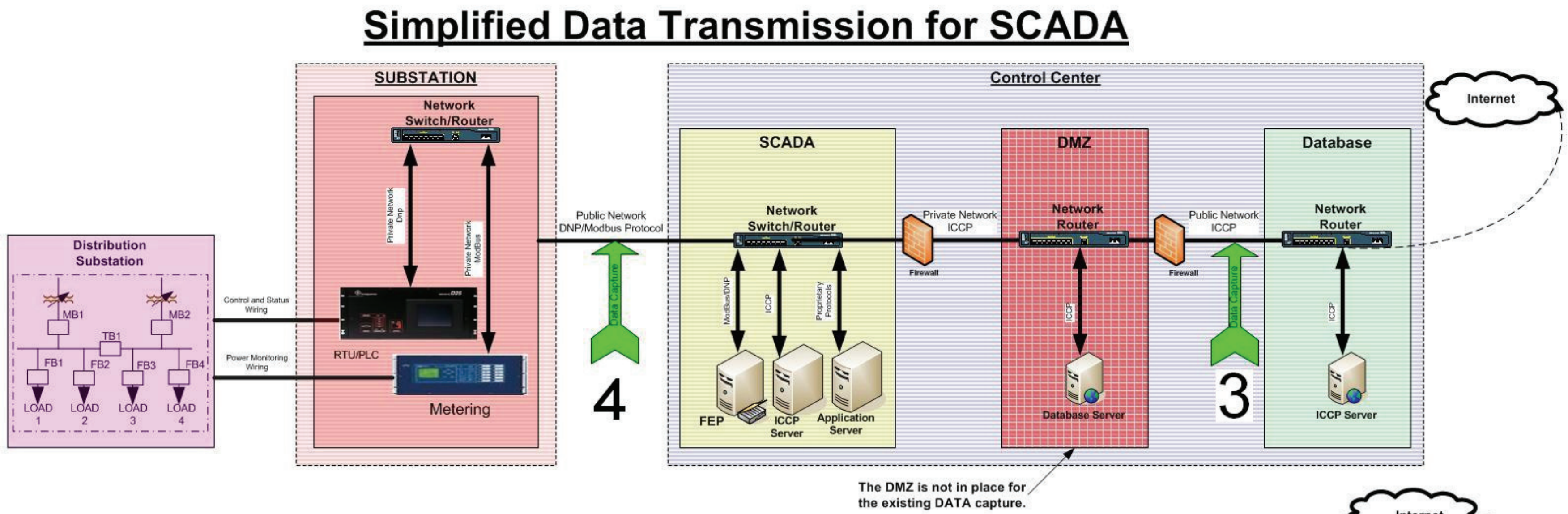
145 bus PDC Data

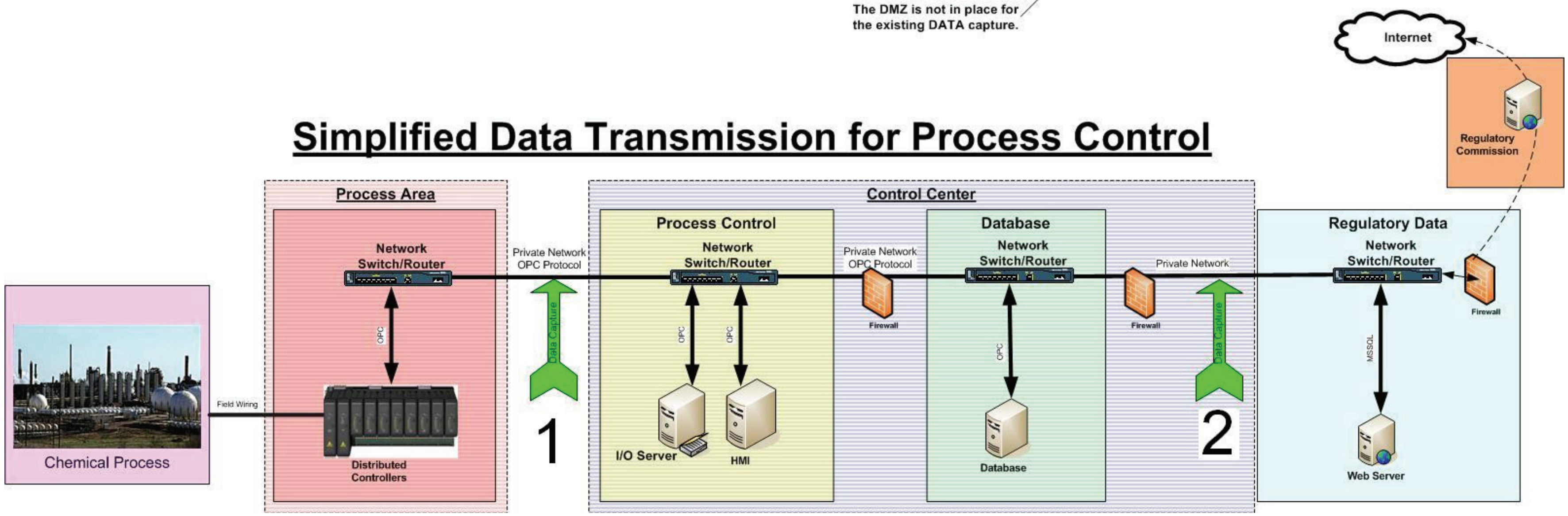
Appendix C - 7

Buses	Branches	Distance	Delay
139	141	778.686	2.597
139	142	29102.215	97.075
139	145	84.436	0.282
140	145	10207.353	34.048
141	115	65.672	0.219
141	116	14710.597	49.069
141	117	34731.27	115.851
141	118	3884.048	12.956
141	131	21868.879	72.947
141	132	152735.027	509.469
141	142	168.872	0.563
141	143	6585.994	21.969
141	144	7092.609	23.658
141	145	356.507	1.189
142	115	1557.372	5.195
142	116	64884.241	216.431
142	117	52500.32	175.122
142	118	1735.625	5.789
142	119	25724.782	85.809
142	120	56693.966	189.111
142	122	24289.372	81.021
142	124	16286.733	54.327
142	125	102261.167	341.107
142	130	33849.384	112.909
142	131	121.963	0.407
142	132	515.997	1.721
142	133	153485.567	511.973
142	143	356.507	1.189
142	144	187.635	0.626
142	145	6923.738	23.095
143	144	45623.491	152.184
144	145	35979.043	120.013

145 bus PDC Data

Appendix D





SCADA data capture

Bibliography

[1] Brendan B. Read. (2010, January) SMARTGRID. [Online]. http://smart-grid.tmcnet.com/topics/smart-grid/articles/72313-new-draft-broadband-over-power-line-standard-published.htm#

[2] Communication Technologies, Inc. (2004, Oct.) National Communications System. [Online]. http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[3] Triangle MicroWorks, Inc. Triangle MicroWorks, Inc. "Solutions for Communication Protocol Development". [Online]. http://www.trianglemicroworks.com/documents/Modbus_and_DNP_Comparison.pdf

[4] Modbus-IDA (Oct). (2006, December) Modbus. [Online]. http://www.modbus-ida.org/docs/PI_MBUS_300.pdf

[5] Modbus-IDA (Dec). (2006, October) Modbus. [Online]. http://www.modbus-ida.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[6] Triangle MicroWorks, Inc. (2002, February) Triangle MicroWorks, Inc. [Online]. http://www.trianglemicroworks.com/documents/DNP3_Overview.pdf

[7] DNP Users Group. (2005, March) Distributed Network Protocol. [Online]. http://www.dnp.org/About/DNP3%20Primer%20Rev%20A.pdf

[8] David Bevin. (2009, September) Control Microsystems. [Online]. http://controlmicrosystems.com/media/page-body-files/white-papers/Modbus_vs_DNP3_whitepaper.pdf

[9] Multitrode Inc. (2007, November) Multitrode (Water, Wastewater, Pump Station, Technology). [Online]. http://www.multitrode.com/download-whitepaper.php?file=uploadFiles/multitrode_12350376811911.pdf

[10] Ming Ding, Yingyuan Zhang, and Meiqin Mao, "Key technologies for microgrids-a review," in *International Conference on Sustainable Power Generation and Supply, 2009*, 2009, pp. 1-5.

[11] IEEE. (2010, June) IEEE. [Online]. http://grouper.ieee.org/groups/scc21/

[12] 109th Congress. (2010, May) Environmental Protection Agency. [Online]. http://www.epa.gov/oust/fedlaws/publ_109-058.pdf

[13] IEEE. (2010, June) IEEE. [Online]. http://grouper.ieee.org/groups/scc21/1547/1547_index.html

[14] IEEE. (2010, June) IEEE. [Online]. http://grouper.ieee.org/groups/scc21/dr_shared/

[15] Amin Abdul and Petru Lupas, "Convergence of Frequency, Time and Data over Ethernet networks," in *ISPCS 2009 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, Brescia, Italy, 2009, pp. 1-5.

[16] Congressional Research Service. (2007, December) United States Senate Committee on Energy & Natural Resources. [Online]. http://energy.senate.gov/public/_files/RL342941.pdf

[17] Department of Energy. Office of Electricity Delivery & Energy Reliability. [Online]. http://www.oe.energy.gov/smartgrid.htm

[18] National Institute of Standards and Technology. (2010, May) National Institute of Standards and Technology, IEEE 1588. [Online]. http://ieee1588.nist.gov/

[19] IEEE. (2007) IEEE Standards Association Working Group Areas. [Online]. http://grouper.ieee.org/groups/1588/

[20] Derek Booth, "A Smart "Smart Grid" Strategy," *Electric Light & Power*, pp. 40-41, Jan/Feb 2008.

[21] Lou Frenzel, "EXPECT MORE CONSUMER BUY-IN BEFORE THE SMART GRID TAKES OFF," *Electronic Design*, pp. 21-23, March 2010.

[22] Synthasite. (2010) smartmeterpedia. [Online]. http://smartmeterpedia.synthasite.com/Enernex_Map.php

[23] The White House. (1998, May) Federation of American Scientists Intelligence Resource Program. [Online]. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

[24] Dong Wei, Yan Lu, Mohsen Jafari, Paul Skare, and Kenneth Rohde, "An Integrated Security System of Protecting Smart Grid against Cyber Attacks," in *Innovative Smart Grid Technologies*, Gaithersburg, 2010, pp. 1-7.

[25] NERC. (2010) North American Electric Reliability Corporation. [Online]. http://www.nerc.com/page.php?cid=1|7|10

[26] NERC. (2010) North American Electric Reliability Corporation. [Online]. http://www.nerc.com/page.php?cid=1|7|11

[27] Allen J. Wood and Bruce F. Wollenberg, *Power Generation Operation and Control*. New York: John Wiley & Sons, Inc., 1996.

[28] Jialnli Pan. (2008, November) A Survey of Network Simulation Tools: Current.

[29] David P. Burton et al. (2009, September) Simulated, Emulated, and Physical Investigative Analysis (SEPIA) of Networked Systems.

[30] Jorge Blasco, "IP-based Standards Support Future Smart Grid," *POWERGRID International*, pp. 60-60, October 2009.

[31] Jean Mahseredjian, Venkata Dinavahi, and Juan A. Martinez, "Simulation Tools for Electromagnetic Transients in Power Systems: Overview and Challenges," *IEEE Transactions on Power Delivery*, pp. 1657-1669, July 2009.

[32] Christian Dufour, Jean Belanger, and Abourida Simon, "Accurate simulation of a 6-pulse inverter with real-time event compensation in ARTEMIS™," *Mathematics & Computers in Simulation*, pp. 161-173, November 2003.

[33] ns-3 development team. (2010, May) ns-3 Tutorial.

[34] T. S. Sidhu and Yujie Yin, "IED Modelling for IEC61850 Based Substation Automation System Performance Simulation," in *2006 Power Engineering Society General Meeting*, Montreal, 2006, pp. 1-7.

[35] Manitoba HVDC Research Centre Inc. (2005, April) EMTDC: The Electromagnetic Transients & Controls Simulation Engine.

[36] Renan Giovanini, Kenneth M. Hopkinson, Denis V. Coury, and James S. Thorp, "A Primary and Backup Cooperative Protection System Based on Wide Area Agents," *IEEE TRANSACTIONS ON POWER DELIVERY*, p. 1222, 2006.

[37] A. Ponti and F. Ponci, "Power Grids of the Future: Why Smart Means Complex," in *COMPENG 2010 Complexity in Engineering*, Rome, 2010, pp. 7-11.

[38] Michael J. Mc Donald, Travis C. Service, Regis H. Cassidy, and Gregory N. Conrad. (2008, September) Cyber Effects Analysis Using VCSE: Promoting Control System Reliability.

[39] University of Washington College of Engineering. Electrical Engineering. [Online]. http://www.ee.washington.edu/research/pstca/

[40] Rich Christie. University of Washington Electrical Engineerig. [Online]. http://www.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm

[41] Renan Giovanini, Kenneth Hopkinson, Denis V. Coury, and James S. Thorp, "A Primary and Backup Cooperative Protection System Based on Wide Area Agents," *IEEE TRANSACTIONS ON POWER DELIVERY*, pp. 1222-1230, 2006.

[42] Juan Carlos_Gonzalez, "An Efficient and Effective Implementation of the Trust System," Air Force Institute of Technology, Wright Patterson AFB, Master's Thesis AFIT/GCS/ENG/09-01, 2009.

[43] Gregory M. Coates, Kenneth M. Hopkinson, Scott R. Graham, and Stuart H. Kurkowski, "Collaborative, Trust-Based Security Mechanisms for a Regional Utility Intranet," *IEEE Transactions on Power Systems*, pp. 831-844, 2008.

[44] Robert S. Cahn, *Wide Area Network Design*. San Francisco: Morgan Kaufmann Pulblishers, Inc., 1998.

[45] OPNET Technologies, Inc. (2011, February) OPNET Modeler/Release 15.0 Chapter 12 - Data Analysis.

[46] Bradley Mitchell. (2011, February) About.com Wireless / Networking. [Online]. http://compnetworking.about.com/od/networkcables/f/t1_t3_lines.htm

[47] Gabriel H. Greve, "NETWORK SECURITY TOOLKIT INCLUDING HEURISTIC SOLUTIONS FOR TRUST SYSTEM PLACEMENT AND NETWORK OBFUSCATION," Air Force Institute of Technology, Wright Patterson AFB, Thesis AFIT/GCS/ENG/10-08, 2010.

[48] Chris Lewis. (2008) Google videos. [Online]. http://video.google.com/videoplay?docid=2323190146585022040#

[49] Spiritus Temporis. (2005) The Spiritus Temporis Web Ring Community. [Online]. http://www.spiritus-temporis.com/high-voltage-direct-current/advantages-of-hvdc-over-ac-transmission.html

[50] Allen J. Wood and Bruce F. Wollenberg, *Power Generation Operation and Control*. New York: John Wiley & Sons, Inc., 1996.

[51] George R. Owens. Energy and Engineering Solutions, Inc. [Online]. http://www.eesienergy.com/10step.shtml

[52] Marshall Brain. (2000, Apr.) How stuff works. [Online]. http://science.howstuffworks.com/power.htm

[53] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *Transmission and Distribution Conference and Exhibition, 2005/2006 IEEE PES*, Dallas, 2006, pp. 376-383.

[54] Klaus P. Brand. (2005, April) CE-B5 Cigre-Brasil. [Online]. http://www.ceb5.cepel.br/arquivos/eventos_setor/iec61850_tutoria.pdf

[55] Jianqing Zhang and Carl A. Gunter. (2009, July) Illinois Security Lab. [Online]. http://seclab.uiuc.edu/docs/iec61850-intro.pdf

[56] NERC. (2010, January) North American Electric Reliability Corporation. [Online]. http://www.nerc.com/files/NEB_CIP_VSL_VRF_filing.pdf

[57] NERC. (2008, April) North American Electric Reliability Corporation. [Online].
http://www.nerc.com/files/Incident-Reporting.pdf

Vita

Captain Marlon C. D. Coerbell graduated from Goshen Central High School in Goshen, New York. Captain Coerbell graduated Cum Laude from Wright State University in 2002. He was commissioned through Officer Training School, Maxwell AFB, Alabama in 2003.

Captain Coerbell has commanded a crew at the Air Force Space Command Network Operations and Security Center, Peterson AFB, Colorado and was Deputy Flight Commander for the Communications Operations Flight, McGuire AFB, New Jersey. Prior to assuming his current position, Captain Coerbell deployed as Communications Projects Officer for Combined Joint Task Force 101, Bagram Air Base, Afghanistan and United States Forces Afghanistan, Kabul, Afghanistan in support of OPERATION ENDURING FREEDOM and the Global War on Terrorism.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
24-03-2011	Master's Thesis	September 2009 – March 2011

TITLE AND SUBTITLE	
Creating a Network Model for the Integration of Dynamic and Static Supervisory Control and Data Acquisition (SCADA) Test Environment	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	**5d. PROJECT NUMBER** 11G222
Coerbell, Marlon C. D., Captain, USAF	**5e. TASK NUMBER**
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)	**8. PERFORMING ORGANIZATION REPORT NUMBER**
Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/ENG) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	AFIT/GCO/ENG/11-02
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** AFOSR/NL
Air Force Office of Scientific Research Attn: Dr. Robert Bonneau 875 N. Randolph St Ste 325 Rm 3112 Arlington, VA 22203 DSN: 426-9545	**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Since 9/11 protecting our critical infrastructure has become a national priority. Presidential Decision Directive 63 mandates and lays a foundation for ensuring all aspects of our nation's critical infrastructure remain secure. Key in this debate is the fact that much of our electrical power grid fails to meet the spirit of this requirement. My research leverages the power afforded by Electric Power and Communication Synchronizing Simulator (EPOCHS) developed with the assistance of Dr. Hopkinson, et al. The power environment is modeled in an electrical simulation environment called PowerWorld©. The network is modeled in OPNET® and populated with self-similar network and Supervisory Control and Data Acquisition (SCADA). The two are merged into one working tool that can realistically model and provide a dynamic network environment coupled with a robust communication methodology. This new suite of tools will enhance the way we model and test hybrid SCADA networks. By combining the best of both worlds we get an effective and robust methodology that correctly predicts the impact of SCADA traffic on a LAN and vice versa. This ability to properly assess data flows will allow professionals in the power industry to develop tools that effectively model future concepts for our critical infrastructure.

15. SUBJECT TERMS
EPOCHS, SCADA, OPNET, PowerWorld, Network, Power, Simulation, Federation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Dr. Kenneth H. Hopkinson (ENG)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
U	U	U	UU	131	(937) 255-6565, ext 4579 (kenneth.hopkinson@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18